الهيئة الوطنية للأمن السيبراني
National Cybersecurity Authority

تمت مشاركة هذه المعلومة بإشارة مشاركة ***أبيض*** حيث يسمح بتبادلها أو نشرها من خلال القنوات العامة.

في ضوء دور الهيئة الوطنية للأمن السيبراني للمساعدة في حماية الفضاء السيبراني الوطني، تود الهيئة مشاركتكم النشرة الأسبوعية للثغرات المسجلة من قبل the National Institute of Standards and Technology (NIST) National Vulnerability Database (NVD) للأسبوع من 5 يوليو إلى 11 يوليو. علماً أنه يتم تصنيف هذه الثغرات باستخدام معيار Common Vulnerability Scoring System (CVSS) حيث يتم تصنيف الثغرات بناء على التالي:

- **عالي جدًا: النتيجة الأساسية لـCVSS 9.0-10.0**
- **عالي: النتيجة الأساسية لـCVSS 7.0-8.9**
- **متوسط: النتيجة الأساسية لـCVSS 4.0-6.9**
- **منخفض: النتيجة الأساسية لـ CVSS 0.0-3.9**

Please note that this notification/advisory has been tagged as TLP ***WHITE*** where information can be shared or published on any public forums.

As part of NCA duties to help securing the cyberspace and protecting national interests, NCA provides the weekly summary of published vulnerabilities by the National Institute of Standards and Technology (NIST) National Vulnerability Database (NVD) for the week from 30th of July to 5th of July. Vulnerabilities are scored using the Common Vulnerability Scoring System (CVSS) standard as per the following severity:

- **Critical: CVSS base score of 9.0-10.0**
- **High: CVSS base score of 7.0-8.9**
- **Medium: CVSS base score 4.0-6.9**
- **Low: CVSS base score 0.0-3.9**

CVE ID & Source	Vendor - Product	Description	Publish Date	CVSS Score
CVE-2026-48316	adobe - multiple products	ColdFusion versions 2025.9, 2023.20 and earlier are affected by an Improper Input Validation vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue does not require user interaction. Scope is changed.	2026-07-06	10
CVE-2026-24014	apache - iotdb	Apache IoTDB DataNode's internal RPC interface for creating Trigger instances uses the uploaded Trigger JAR name to build a file path without sufficient validation. If the internal DataNode RPC port is exposed to an untrusted network, an attacker may use path traversal sequences in the JAR name to write files outside the intended Trigger installation directory. This could allow arbitrary file write with the permissions of the IoTDB process. This issue affects Apache IoTDB: from 1.3.3 before 2.0.8. Users are recommended to upgrade to version 2.0.8, which fixes the issue.	2026-07-06	9.8
CVE-2026-43867	apache - multiple products	Deserialization of Untrusted Data vulnerability in Apache Camel PQC Component. The camel-pqc component persists post-quantum key metadata (KeyMetadata) through pluggable KeyLifecycleManager implementations. AwsSecretsManagerKeyLifecycleManager.deserializeMetadata() reads that metadata back from the configured AWS Secrets Manager secret by Base64-decoding the stored value and deserializing it with a raw java.io.ObjectInputStream.readObject() and no ObjectInputFilter or class allow-list; the cast to KeyMetadata happens only after readObject() returns, so any readObject() side effects in a crafted object run before the type check. A principal who can write to the AWS Secrets Manager secret that holds this metadata (requiring secretsmanager:PutSecretValue on that secret) could store a crafted serialized object that is deserialized during normal key-lifecycle operations, potentially leading to code execution in the context of the application that manages the keys. This is the same underlying defect, in the same code path and remediated by the same fix, as CVE-2026-46590, which was reported independently and additionally covers the HashiCorp Vault and file-based sibling managers; both are incomplete-remediation follow-ons to CVE-2026-40048 (CAMEL-23200). This issue affects Apache Camel: from 4.18.0 before 4.18.3, from 4.19.0 before 4.21.0. Users are recommended to upgrade to version 4.21.0, which fixes the issue. If users are on the 4.18.x LTS releases stream, then they are suggested to upgrade to 4.18.3. For deployments that cannot upgrade immediately, restrict write access to the AWS Secrets Manager secret that holds the camel-pqc key metadata so that only the application's own identity holds secretsmanager:PutSecretValue on it (least-privilege IAM), and keep the PQC key material in a secret separate from any data that less-trusted principals can write.	2026-07-06	9.8
CVE-2026-46454	apache - multiple products	Improper Input Validation vulnerability in Apache Camel Cometd Component. The camel-cometd component maps inbound Bayeux (CometD) message headers into the Camel Exchange without applying a HeaderFilterStrategy. CometdBinding.populateExchangeFromMessage copies the entire ext.CamelHeaders map supplied by the CometD client directly onto the Camel message (message.setHeaders), so any header name - including Camel-internal control headers such as CamelHttpUri, CamelFileName or CamelJmsDestinationName - is accepted unmodified. Because a CometdComponent installs no Bayeux SecurityPolicy by default, any client that can complete the Bayeux handshake against the CometD endpoint can publish such a message without authentication. An attacker can therefore inject arbitrary Camel control headers that influence	2026-07-06	9.8

		the behaviour of downstream producers in the route (for example redirecting an HTTP producer, changing a file name, or overriding a JMS destination); the injected headers also persist across internal direct, seda and vm hops. The concrete downstream impact depends on which producers the route uses. This issue affects Apache Camel: from 4.0.0 before 4.14.8, from 4.15.0 before 4.18.3, from 4.19.0 before 4.21.0. Users are recommended to upgrade to version 4.21.0, which fixes the issue. If users are on the 4.14.x LTS releases stream, then they are suggested to upgrade to 4.14.8. If users are on the 4.18.x releases stream, then they are suggested to upgrade to 4.18.3. The fix implements a HeaderFilterStrategy in the camel-cometd binding (a long-standing TODO in the code) that filters the Camel header namespace case-insensitively on inbound mapping, so client-supplied Camel* / camel* headers are no longer copied into the Exchange. For deployments that cannot upgrade immediately, strip the Camel control headers from inbound CometD messages before they reach any downstream producer (for example removeHeaders('Camel*') and removeHeaders('camel*') at the start of the route), and install an explicit Bayeux SecurityPolicy on the CometdComponent so that only authenticated clients can publish.		
CVE-2026-46455	apache - multiple products	Insufficient Session Expiration vulnerability in Apache Camel Keycloak Component. The camel-keycloak security helper KeycloakSecurityHelper.parseAndVerifyAccessToken builds a Keycloak TokenVerifier using withChecks(...) with only the subject-exists check and the realm-URL (issuer) check. Keycloak's TokenVerifier.withChecks(...) appends to an initially empty check list - the upstream default checks are installed only when withDefaultChecks() is called - so the built-in IS_ACTIVE predicate, which validates the token's exp (expiration) and nbf (not-before) claims, is never applied. As a result the helper verifies the token signature, subject and issuer but does not enforce the token's validity window: an access token that is expired, or not yet valid, is accepted as valid. Routes that rely on this helper to authenticate inbound requests therefore accept access tokens that are outside their intended lifetime. This issue affects Apache Camel: from 4.18.0 before 4.18.3, from 4.19.0 before 4.21.0. Users are recommended to upgrade to version 4.21.0, which fixes the issue. If users are on the 4.18.x releases stream, then they are suggested to upgrade to 4.18.3. The fix makes KeycloakSecurityHelper.parseAndVerifyAccessToken include the TokenVerifier.IS_ACTIVE check so that expired or not-yet-valid access tokens are rejected, aligning the helper with Keycloak's default check set. For deployments that cannot upgrade immediately, enforce token expiration outside the helper - for example validate the access token's exp/nbf claims in the route before trusting it, keep Keycloak access-token lifetimes short, and ensure any upstream gateway or resource server also validates the token validity window.	2026-07-06	9.8
CVE-2026-46456	apache - multiple products	Improper Input Validation vulnerability in Apache Camel AWS2-SQS Component. The camel-aws2-sqs component map inbound message attributes into the Camel Exchange through a component-specific HeaderFilterStrategy. Sqs2HeaderFilterStrategy configured only an outbound filter (setOutFilterPattern, which blocks Camel*, breadcrumbId and org.apache.camel.* headers being written to the broker) but did not configure an inbound filter. As a result, when Sqs2Consumer copies each SQS MessageAttribute into the Exchange via HeaderFilterStrategy.applyFilterToExternalHeaders, DefaultHeaderFilterStrategy applied no inbound rule and treated every header name as not filtered - including Camel-internal control headers such as CamelHttpUri, CamelFileName or CamelSqlQuery - copying them unmodified onto the Camel message. Any principal able to send messages to the consumed SQS queue (for example a cross-account sender or a lower-privileged in-account component holding sqs:SendMessage) could therefore set arbitrary Camel control headers that influence the behaviour of downstream producers in the route (for example redirecting an HTTP producer, changing a file name, or overriding a query); the injected headers also persist across internal direct, seda and vm hops. The concrete downstream impact depends on which producers the route uses. This issue affects Apache Camel: from 4.0.0 before 4.14.8, from 4.15.0 before 4.18.3, from 4.19.0 before 4.21.0. Users are recommended to upgrade to version 4.21.0, which fixes the issue. If users are on the 4.14.x LTS releases stream, then they are suggested to upgrade to 4.14.8. If users are on the 4.18.x releases stream, then they are suggested to upgrade to 4.18.3. The fix adds an inbound HeaderFilterStrategy rule to Sqs2HeaderFilterStrategy that filters the Camel header namespace case-insensitively on inbound mapping, so sender-supplied Camel* / camel* headers are no longer copied into the Exchange. For deployments that cannot upgrade immediately, strip the Camel control headers from inbound messages before they reach any downstream producer (for example removeHeaders('Camel*') and removeHeaders('camel*') at the start of the route), and restrict who may send to the consumed SQS queue by applying least-privilege sqs:SendMessage permissions on the queue resource policy.	2026-07-06	9.8
CVE-2026-48204	apache - multiple products	Improper Input Validation, Improper Access Control vulnerability in Apache Camel in Camel Mongodb Gridfs component. The camel-mongodb-gridfs producer selects the GridFS operation to perform from the gridfs.operation Exchange header when the endpoint's operation parameter is not set - which is the default. The control-header constants (GridFsConstants.GRIDFS_OPERATION, GRIDFS_OBJECT_ID, GRIDFS_METADATA, GRIDFS_CHUNKSIZE, GRIDFS_FILE_ID_PRODUCED) were the plain strings gridfs.operation, gridfs.objectid, gridfs.metadata, gridfs.chunksize and gridfs.fileid. Because these names do not start with the Camel / camel prefix, HttpHeaderFilterStrategy - which blocks only the Camel header namespace on the HTTP	2026-07-06	9.8

		boundary - let them pass from an inbound HTTP request straight into the Exchange. In a route that bridges an HTTP consumer (for example platform-http) into a mongodb-gridfs: producer with no explicit operation, any HTTP client could therefore set the gridfs.operation header to override the route's intended operation - switching, for example, a file upload to remove (deleting a file identified by the attacker-supplied gridfs.objectid), listAll (enumerating every file in the bucket) or findOne (reading a file) - and supply a gridfs.metadata value that is parsed as a MongoDB document, enabling NoSQL operator injection. No credentials are required when the bridging consumer is unauthenticated. This issue affects Apache Camel: from 4.0.0 before 4.14.8, from 4.15.0 before 4.18.3, from 4.19.0 before 4.21.0. Users are recommended to upgrade to version 4.21.0, which fixes the issue. If users are on the 4.14.x LTS releases stream, then they are suggested to upgrade to 4.14.8. If users are on the 4.18.x releases stream, then they are suggested to upgrade to 4.18.3. After upgrading, routes that drive GridFS operations or metadata via the raw header names must use CamelGridFsOperation / CamelGridFsObjectId / CamelGridFsMetadata / CamelGridFsChunkSize / CamelGridFsFileId instead of the gridfs.* names. For deployments that cannot upgrade immediately, set an explicit operation on the mongodb-gridfs: endpoint so the operation is not taken from a header, and strip the gridfs.* headers from any untrusted ingress before the producer.		
CVE-2026-53913	apache - multiple products	Improper Authentication, Missing Authentication for Critical Function, Not Failing Securely ('Failing Open') vulnerability in Apache Camel Keycloak Component. The KeycloakSecurityPolicy of camel-keycloak guards a route by running KeycloakSecurityProcessor.beforeProcess(), which performs three checks in sequence: it rejects a request that carries no access token, then - only if requiredRoles is non-empty - validates the roles, and - only if requiredPermissions is non-empty - validates the permissions. The actual cryptographic verification of the bearer access token (signature, issuer and expiry for a local JWT, or active-state and issuer for token introspection) is performed exclusively inside those role and permission checks. KeycloakSecurityPolicy defaults requiredRoles and requiredPermissions to empty - which is the documented 'Basic Setup' - so on a route configured that way the role and permission checks are skipped and the access token is therefore never verified. The token-presence check still rejects a missing token, but an invalid token is accepted: any non-null value in the Authorization: Bearer header - including an arbitrary string or a forged, unsigned JWT - passes the policy and the request reaches the protected route, with no signature, issuer or expiry check and no request to Keycloak. The token is read from the inbound request header because allowTokenFromHeader defaults to true. Because the normal reason to place a route behind this policy is that the route performs server-side work, the bypass results in unauthenticated access to that work; where the protected route forwards to a code-execution-capable producer, it can result in unauthenticated remote code execution. This defect is independent of CVE-2026-23552: that issue concerned the issuer claim and was fixed by adding a check inside the verification routine, but here the verification routine is not reached at all in the default configuration, so the defect remains. This issue affects Apache Camel: from 4.15.0 before 4.18.3, from 4.19.0 before 4.21.0. Users are recommended to upgrade to version 4.21.0, which fixes the issue. If users are on the 4.18.x releases stream, then they are suggested to upgrade to 4.18.3. For deployments that cannot upgrade immediately, configure a non-empty requiredRoles or requiredPermissions on every KeycloakSecurityPolicy so that the token-verification path is exercised, set allowTokenFromHeader to false where the token is not expected from the request header, or perform token verification at the framework layer ahead of the policy.	2026-07-06	9.8
CVE-2026-56140	apache - multiple products	Improper Input Validation vulnerability in Apache Camel AWS SNS component. The camel-aws2-sns component filters Camel headers through a component-specific HeaderFilterStrategy, Sns2HeaderFilterStrategy. Like the sibling Sqs2HeaderFilterStrategy, it originally configured only an outbound filter (setOutFilterPattern, which blocks Camel*, breadcrumbId and org.apache.camel.* headers from being written out) and did not configure an inbound filter rule. For the related camel-aws2-sqs component this inbound gap was exploitable, because the Sqs2Consumer maps inbound SQS message attributes into the Camel Exchange via HeaderFilterStrategy.applyFilterToExternalHeaders, allowing a message sender to inject Camel control headers (tracked as CVE-2026-46456). camel-aws2-sns, by contrast, is producer-only: Sns2Endpoint does not support consumers (createConsumer throws UnsupportedOperationException, 'You cannot receive messages from this endpoint'), so no externally-supplied message attributes are ever mapped inbound into a Camel Exchange through SNS, and the missing inbound filter rule on Sns2HeaderFilterStrategy was therefore not reachable by an attacker. As part of the same fix (CAMEL-23506), an inbound filter rule (setInFilterStartsWith for the Camel namespace) was added to Sns2HeaderFilterStrategy so that its configuration matches the corrected Sqs2HeaderFilterStrategy and the other sibling strategies. This is a defense-in-depth alignment with no known exploit path in camel-aws2-sns. This issue affects Apache Camel: from 4.0.0 before 4.14.8, from 4.15.0 before 4.18.3, from 4.19.0 before 4.21.0. This is a defense-in-depth hardening change with no known exploit path in camel-aws2-sns, which is producer-only, so no urgent action or workaround is required. Users who want the aligned behaviour can upgrade to version 4.21.0, or to 4.14.8 on the 4.14.x LTS releases stream, or to 4.18.3 on the 4.18.x releases stream, which contain the change. As a general	2026-07-06	9.8

		best practice, operators should continue to apply least-privilege IAM permissions on their SNS topics.		
CVE-2026-33264	apache - airflow	A bug in `BaseSerialization.deserialize()` allowed unrestricted `import_string()` of attacker-controlled class paths when the Scheduler / API Server loaded a serialized DAG: a DAG author could embed a malicious trigger into a DAG to gain remote code execution on the API Server / Scheduler process, crossing the Airflow security boundary that DAG-author code must never execute in those processes. Users are advised to upgrade to `apache-airflow` 3.3.0 or later. As a defense-in-depth mitigation, deployments where DAG-author trust is limited can restrict the `[core] allowed_deserialization_classes` config to a narrow allowlist.	2026-07-07	9.8
CVE-2026-53481	dell - multiple products	Dell PowerProtect Data Domain, versions 7.7.1.0 through 8.7, LTS2026 release version 8.6.1.0 through 8.6.1.10, LTS2025 release version 8.3.1.0 through 8.3.1.30, LTS2024 release versions 7.13.1.0 through 7.13.1.70 contain an improper limitation of a pathname to a restricted directory ('Path Traversal') vulnerability. An unauthenticated attacker with remote access could potentially exploit this vulnerability, leading to unauthorized access to the system. This is a critical severity vulnerability as it allows an attacker to take complete control of system; so Dell recommends customers to upgrade at the earliest opportunity.	2026-07-07	9.8
CVE-2026-53483	dell - multiple products	Dell PowerProtect Data Domain, versions 7.7.1.0 through 8.7, LTS2026 release version 8.6.1.0 through 8.6.1.10, LTS2025 release version 8.3.1.0 through 8.3.1.30, LTS2024 release versions 7.13.1.0 through 7.13.1.70 an improper authentication vulnerability. An unauthenticated attacker with remote access could potentially exploit this vulnerability, leading to unauthorized access. This is a critical severity vulnerability as it allows an attacker to take complete control of system; so Dell recommends customers to upgrade at the earliest opportunity.	2026-07-07	9.8
CVE-2026-28564	apache software foundation - Apache IoTDB	Insufficient Session Expiration, Authentication Bypass by Capture-replay vulnerability in Apache IoTDB. REST Basic Authentication Accepts Stale Cached Credentials This issue affects Apache IoTDB: from 1.0.0 before 2.0.10. Users are recommended to upgrade to version 2.0.10, which fixes the issue.	2026-07-10	9.8
CVE-2026-40008	apache software foundation - Apache IoTDB	Use of Externally-Controlled Input to Select Classes or Code ('Unsafe Reflection') vulnerability in Apache IoTDB. The pipe processor reads a fully qualified Java class name and instantiates it using Class.forName().newInstance() without any validation or allowlisting. This issue affects Apache IoTDB: from 1.0.0 before 2.0.10. Users are recommended to upgrade to version 2.0.10, which fixes the issue.	2026-07-10	9.8
CVE-2026-53363	linux - multiple products	In the Linux kernel, the following vulnerability has been resolved: xfrm: iptfs: preserve shared-frag marker in iptfs_consume_frags() iptfs_consume_frags() transfers paged fragments from one socket buffer to another but fails to propagate the SKBFL_SHARED_FRAG flag. This is the same class of bug that was fixed in skb_try_coalesce() for CVE-2026-46300: when fragments backed by read-only page-cache pages are merged, the marker indicating their shared nature must be preserved so that ESP can decide correctly whether in-place encryption is safe. Apply the same two-line fix used in skb_try_coalesce() to iptfs_consume_frags().	2026-07-10	9.8
CVE-2026-9726	drupal - Drupal AlternativeCommerce (Basket)	Improperly Controlled Modification of Dynamically-Determined Object Attributes vulnerability in Drupal Drupal AlternativeCommerce (Basket) allows Object Injection. This issue affects Drupal AlternativeCommerce (Basket) versions: from 0.0.0 to 2.1.17.	2026-07-10	9.8
CVE-2026-10768	drupal - LocalGov Workflows	Missing Authorization vulnerability in Drupal LocalGov Workflows allows Forceful Browsing. This issue affects LocalGov Workflows versions: from 0.0.0 to 1.6.0.	2026-07-10	9.8
CVE-2026-12535	drupal - Formatter Field	Improperly Controlled Modification of Dynamically-Determined Object Attributes vulnerability in Drupal Formatter Field allows Object Injection. This issue affects Formatter Field versions: from 0.0.0 to 2.0.0.	2026-07-10	9.8
CVE-2026-11913	drupal - Mother May I	vulnerability in Drupal Mother May I allows . This issue affects Mother May I versions: *.*.	2026-07-10	9.8
CVE-2026-15113	google - chrome	Use after free in Autofill in Google Chrome on Android prior to 150.0.7871.115 allowed a remote attacker to potentially perform a sandbox escape via a crafted HTML page. (Chromium security severity: High)	2026-07-08	9.6
CVE-2026-47646	microsoft - dynamics_365_customer_voice	Improper neutralization of input during web page generation ('cross-site scripting') in Dynamics 365 Customer Voice allows an unauthorized attacker to perform spoofing over a network.	2026-07-09	9.3
CVE-2026-15378	red hat - Red Hat OpenShift AI (RHOAI)	A flaw was found in the `guardrails-detectors` component. This vulnerability allows a remote attacker to perform a blind Server-Side Request Forgery (SSRF) by submitting a specially crafted XML Schema Definition (XSD) string. This can lead to unauthorized access to sensitive information, including credentials from cloud metadata services, Kubernetes API, internal MinIO, and other internal network endpoints. Additionally, it enables local file reads of critical data such as service account tokens and pod secrets.	2026-07-10	9.3
CVE-2026-15143	red hat - multiple products	A flaw was found in the file_type content detector of guardrails-detectors. This vulnerability allows a remote attacker to supply an arbitrary XML Schema Definition (XSD) string, which is processed without proper restrictions. This can lead to server-side requests to arbitrary URLs	2026-07-10	9.3

		or local file reads, potentially resulting in sensitive information disclosure, such as cloud provider credentials or access to internal network services.		
CVE-2026-24013	apache - iotdb	Authentication Bypass by Spoofing vulnerability in Apache IoTDB. Certain Thrift RPC query handlers lack strict validation of the sessionId parameter. An attacker can construct requests with a forged sessionId and, without performing openSession authentication, receive valid query results. This allows authentication bypass and unauthorized reading of time-series data. This issue affects Apache IoTDB: from 1.3.3 before 2.0.8. Users are recommended to upgrade to version 2.0.8, which fixes the issue.	2026-07-06	9.1
CVE-2026-40047	apache - camel	Improper Neutralization of Argument Delimiters in a Command ('Argument Injection') vulnerability in Apache Camel Docling component. The camel-docling component invokes the external `docling` command-line tool by assembling an argument list in DoclingProducer and executing it through java.lang.ProcessBuilder. Custom CLI arguments supplied through the `CamelDoclingCustomArguments` exchange header (a List<String>) were appended to that argument list with insufficient validation: the original implementation relied on a denylist of disallowed flags and only rejected path values that contained a literal `../` sequence. As a result, a Camel route that forwards externally-influenced data into the `CamelDoclingCustomArguments` header (or into the path-bearing headers used to build the invocation) could cause the producer to pass unrecognized or unintended `docling` CLI flags to the subprocess, and could supply path-like argument values that resolved outside the intended directory through traversal sequences not caught by the literal `../` check. Because Camel itself builds the `docling` invocation from these values, the component is responsible for constraining them, and the weak validation allowed CLI-argument injection and directory traversal in the arguments passed to the external tool. The invocation uses the list-based form of ProcessBuilder, so a shell does not interpret the argument values; OS command injection through shell metacharacters was not possible, and the metacharacter rejection added by the fix is defense-in-depth. This issue affects Apache Camel: from 4.15.0 before 4.18.3. Users are recommended to upgrade to a release that contains the CAMEL-23212 fix. On the mainline the fix is included from Apache Camel 4.19.0 (and later releases such as 4.20.0). For users on the 4.18.x LTS releases stream, upgrade to 4.18.3. The fix replaces the denylist with a strict allowlist of recognized `docling` CLI flags (rejecting any unrecognized flag, and rejecting producer-managed flags such as the output-directory flags), defensively rejects shell metacharacters in argument values, and normalizes path-like values with Path.normalize() before validating them so that traversal sequences which bypass a literal `../` check are detected. As defence in depth, route authors should avoid mapping untrusted message content into the `CamelDoclingCustomArguments` header and the path-bearing headers, and should strip Camel-internal headers from messages that arrive from untrusted producers.	2026-07-06	9.1
CVE-2026-48203	apache - multiple products	Improper Neutralization of Special Elements in Output Used by a Downstream Component ('Injection'), Improper Input Validation, Server-Side Request Forgery (SSRF) vulnerability in Apache Camel Solr component. The camel-solr producer copies Exchange message headers whose names begin with the SolrParam. prefix into the parameters of the Solr request, and headers whose names begin with the SolrField. prefix into the fields of the indexed Solr document. The prefix constants (SolrConstants.HEADER_PARAM_PREFIX / HEADER_FIELD_PREFIX) were the plain strings SolrParam. / SolrField.. Because these names do not start with the Camel / camel prefix, HttpHeaderFilterStrategy - which blocks only the Camel header namespace on the HTTP boundary - let them pass from an inbound HTTP request straight into the Exchange. In a route that bridges an HTTP consumer (for example platform-http) into a solr: producer, any HTTP client could therefore set SolrParam.* headers to inject arbitrary Solr request parameters - including shards or stream.url, which cause the Solr server to issue server-side requests to an attacker-chosen URL (server-side request forgery, for example to an internal service or a cloud metadata endpoint), or qt to reach administrative request handlers - and set SolrField.* headers to inject arbitrary fields into indexed documents. No credentials are required when the bridging consumer is unauthenticated. This issue affects Apache Camel: from 4.0.0 before 4.14.8, from 4.15.0 before 4.18.3, from 4.19.0 before 4.21.0. Users are recommended to upgrade to version 4.21.0, which fixes the issue. If users are on the 4.14.x LTS releases stream, then they are suggested to upgrade to 4.14.8. If users are on the 4.18.x releases stream, then they are suggested to upgrade to 4.18.3. After upgrading, routes that set Solr parameters or fields via the raw header prefixes must use CamelSolrParam. / CamelSolrField. instead of SolrParam. / SolrField.. For deployments that cannot upgrade immediately, strip the SolrParam.* and SolrField.* headers from any untrusted ingress before the solr: producer, and set the required Solr parameters and fields from a trusted source in the route.	2026-07-06	9.1
CVE-2026-48205	apache - multiple products	Improper Input Validation, Server-Side Request Forgery (SSRF) vulnerability in Apache Camel DNS component. The camel-dns producers read DNS operation parameters - the resolver to query, the name or domain to look up, the record type and class, and the search term - from Exchange message headers whose constant values (DnsConstants.DNS_SERVER, DNS_NAME, DNS_DOMAIN, DNS_TYPE, DNS_CLASS, TERM) were the plain strings dns.server, dns.name, dns.domain,	2026-07-06	9.1

		dns.type, dns.class and term. Because these names do not start with the Camel / camel prefix, HttpHeaderFilterStrategy - which blocks only the Camel header namespace on the HTTP boundary - let them pass from an inbound HTTP request straight into the Exchange. In a route that bridges an HTTP consumer (for example platform-http) into a dns: producer, any HTTP client could therefore set the dns.server header to make the dig producer build a SimpleResolver pointing at an attacker-controlled DNS server - a server-side request forgery via DNS, through which the attacker observes the queried name and can return poisoned responses - and set the dns.name / dns.domain headers to resolve arbitrary internal hostnames, disclosing whether they exist (internal network reconnaissance). No credentials are required when the bridging consumer is unauthenticated. This issue affects Apache Camel: from 4.0.0 before 4.14.8, from 4.15.0 before 4.18.3, from 4.19.0 before 4.21.0. Users are recommended to upgrade to version 4.21.0, which fixes the issue. If users are on the 4.14.x LTS releases stream, then they are suggested to upgrade to 4.14.8. If users are on the 4.18.x releases stream, then they are suggested to upgrade to 4.18.3. After upgrading, routes that drive DNS operations via the raw header names must use CamelDnsServer / CamelDnsName / CamelDnsDomain / CamelDnsType / CamelDnsClass / CamelDnsTerm instead of the dns.* / term names. For deployments that cannot upgrade immediately, strip the dns.* and term headers from any untrusted ingress before the dns: producer, and set the DNS server and lookup parameters from a trusted source in the route.		
CVE-2026-41042	apache software foundation - Apache Gravitino	Unauthenticated callers can supply a malicious H2 JDBC URL through the testConnection API, which executes arbitrary Java code on the server via H2's INIT parameter. Vulnerability in Apache Gravitino. This issue affects Apache Gravitino: before 1.2.1. Users are recommended to upgrade to version 1.2.1, which fixes the issue. This issue only happens when using H2, and H2 is mainly used for testing and local development. Also, Gravitino is typically deployed in the internal environment, so the severity is low.	2026-07-08	9.1
CVE-2026-9074	ibm - multiple products	IBM API Connect 10.0.8.0 through 10.0.8.9 and 12.1.0.0 through 12.1.0.3 contains an unauthenticated SQL injection vulnerability in the password reset functionality.	2026-07-08	9.1
CVE-2026-40005	apache software foundation - Apache IoTDB	Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal') vulnerability in Apache IoTDB. An attacker can write arbitrary files anywhere the IoTDB process has write permissions with unsafe API. This issue affects Apache IoTDB: from 1.0.0 before 2.0.10. Users are recommended to upgrade to version 2.0.10, which fixes the issue.	2026-07-10	9.1
CVE-2026-56688	dell - multiple products	Dell PowerFlex Manager, Version prior to 5.1.0.1, contain(s) an Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection') vulnerability. A high privileged attacker with remote access could potentially exploit this vulnerability during OS Repository processing to achieve arbitrary command execution as root, potentially leading to full appliance compromise and lateral movement into managed infrastructure.	2026-07-10	9.1
CVE-2026-15089	drupal - Commerce guest registration	vulnerability in Drupal Commerce guest registration allows . This issue affects Commerce guest registration versions: *.*.	2026-07-10	9.1
CVE-2026-46590	apache - multiple products	Deserialization of Untrusted Data vulnerability in Apache Camel PQC component. The camel-pqc component persists post-quantum key metadata (KeyMetadata) through pluggable KeyLifecycleManager implementations. HashicorpVaultKeyLifecycleManager and AwsSecretsManagerKeyLifecycleManager read that metadata back from the configured secret backend by deserializing a Base64-wrapped value with a raw java.io.ObjectInputStream.readObject() and no ObjectInputFilter or class allow-list; the cast to KeyMetadata happens only after readObject() returns, so any readObject() side effects in a crafted object run before the type check. The same unfiltered legacy-migration read also remained in FileBasedKeyLifecycleManager (for the stored KeyPair and KeyMetadata). A principal who can write to the operator-controlled backend that holds these values - the HashiCorp Vault KV path, or the AWS Secrets Manager secret (requiring a Vault token or secretsmanager:PutSecretValue) - could store a crafted serialized object that is deserialized during normal key-lifecycle operations, potentially leading to code execution in the context of the application that manages the keys. This is an incomplete-remediation follow-on to CVE-2026-40048 (CAMEL-23200), which changed FileBasedKeyLifecycleManager to store metadata as JSON / PKCS#8 / X.509 but did not add an ObjectInputFilter, did not cover the Vault and AWS sibling managers, and left FileBasedKeyLifecycleManager's own legacy-migration deserialization unfiltered. This issue affects Apache Camel: from 4.18.0 before 4.18.3, from 4.19.0 before 4.21.0. Users are recommended to upgrade to version 4.21.0, which fixes the issue. If users are on the 4.18.x LTS releases stream, then they are suggested to upgrade to 4.18.3. For deployments that cannot upgrade immediately, restrict write access to the key backend so that only the application's own identity can write the camel-pqc secrets (least-privilege HashiCorp Vault policies and secretsmanager:PutSecretValue IAM), and keep the PQC key material in a backend separate from any data that less-trusted principals can write.	2026-07-06	8.8
CVE-2026-25268	qualcomm - wsa8835_firmware	Memory Corruption when processing invalid HT40 channel layouts during dynamic channel switching operations.	2026-07-06	8.8

CVE-2026-14474	red hat - multiple products	A flaw was found in SSSD's LDAP sudo provider. When the ldap_sudo_search_base option is not explicitly configured, SSSD searches the entire LDAP directory tree for sudoRole objects. An authenticated attacker with write access to any subtree can inject a sudoRole object granting root-level sudo privileges on all SSSD-enrolled hosts.	2026-07-07	8.8
CVE-2026-56086	dell - multiple products	Dell PowerProtect Data Domain, versions 7.7.1.0 through 8.6, LTS2026 release version 8.6.1.0 through 8.6.1.10, LTS2025 release version 8.3.1.0 through 8.3.1.30, LTS2024 release versions 7.13.1.0 through 7.13.1.70 contain an Incorrect Authorization vulnerability. A low privileged attacker with remote access could potentially exploit this vulnerability, leading to unauthorized access.	2026-07-08	8.8
CVE-2026-15107	google - chrome	Use after free in IndexedDB in Google Chrome prior to 150.0.7871.115 allowed a remote attacker to execute arbitrary code inside a sandbox via a crafted HTML page. (Chromium security severity: Medium)	2026-07-08	8.8
CVE-2026-15110	google - chrome	Use after free in Extensions in Google Chrome prior to 150.0.7871.115 allowed an attacker who convinced a user to install a malicious extension to potentially exploit heap corruption via a crafted Chrome Extension. (Chromium security severity: High)	2026-07-08	8.8
CVE-2026-15112	google - chrome	Use after free in Ozone in Google Chrome prior to 150.0.7871.115 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. (Chromium security severity: Critical)	2026-07-08	8.8
CVE-2026-15114	google - chrome	Out of bounds read and write in Codecs in Google Chrome prior to 150.0.7871.115 allowed a remote attacker to potentially exploit heap corruption via a crafted video file. (Chromium security severity: High)	2026-07-08	8.8
CVE-2026-15116	google - chrome	Use after free in Actor in Google Chrome prior to 150.0.7871.115 allowed a remote attacker to execute arbitrary code inside a sandbox via a crafted HTML page. (Chromium security severity: High)	2026-07-08	8.8
CVE-2026-15118	google - chrome	Use after free in Input in Google Chrome prior to 150.0.7871.115 allowed a remote attacker to execute arbitrary code inside a sandbox via a crafted HTML page. (Chromium security severity: High)	2026-07-08	8.8
CVE-2026-15121	google - chrome	Use after free in WebRTC in Google Chrome prior to 150.0.7871.115 allowed a remote attacker to execute arbitrary code inside a sandbox via a crafted HTML page. (Chromium security severity: High)	2026-07-08	8.8
CVE-2026-15123	google - chrome	Inappropriate implementation in DOM in Google Chrome prior to 150.0.7871.115 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. (Chromium security severity: High)	2026-07-08	8.8
CVE-2026-15125	google - chrome	Inappropriate implementation in Forms in Google Chrome prior to 150.0.7871.115 allowed a remote attacker to execute arbitrary code inside a sandbox via a crafted HTML page. (Chromium security severity: High)	2026-07-08	8.8
CVE-2026-15126	google - chrome	Use after free in Forms in Google Chrome prior to 150.0.7871.115 allowed a remote attacker to execute arbitrary code inside a sandbox via a crafted HTML page. (Chromium security severity: High)	2026-07-08	8.8
CVE-2026-15129	google - chrome	Use after free in Views in Google Chrome prior to 150.0.7871.115 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. (Chromium security severity: Critical)	2026-07-08	8.8
CVE-2026-15132	google - chrome	Uninitialized Use in V8 in Google Chrome prior to 150.0.7871.115 allowed a remote attacker to execute arbitrary code inside a sandbox via a crafted HTML page. (Chromium security severity: High)	2026-07-08	8.8
CVE-2026-15133	google - chrome	Use after free in InterestGroups in Google Chrome prior to 150.0.7871.115 allowed a remote attacker to execute arbitrary code inside a sandbox via a crafted HTML page. (Chromium security severity: High)	2026-07-08	8.8
CVE-2026-54469	dell - unisphere_for_powermax	Dell Unisphere for PowerMax, version(s) 10.3.0.5 and prior, contain(s) a Deserialization of Untrusted Data vulnerability. A low privileged attacker with remote access could potentially exploit this vulnerability, leading to arbitrary command execution with root privileges.	2026-07-10	8.8
CVE-2026-58469	gnu - wget	GNU Wget through 1.25.0, fixed in commit 37a40fc, contains a heap buffer underread vulnerability in the clean_metalink_string() function within src/metalink.c that allows a malicious server to trigger memory corruption by serving a Metalink document containing a whitespace-only URL. Attackers can cause the function to decrement a pointer past the start of the buffer when processing an all-whitespace Metalink URL, potentially leading to abnormal program behavior.	2026-07-07	8.7
CVE-2026-57023	juniper - multiple products	An Improper Validation of Specified Quantity in Input vulnerability in the TCP proxy plugin of Juniper Networks Junos OS on MX Series with SPC3, and SRX Series allows an unauthenticated, network-based attacker to cause a complete Denial of Service (DoS). When TCP proxy is engaged in a flow session, to support ALGs, Advanced Anti-Malware, ICAP or UTM, a TCP packet with specifically malformed TCP header will cause flow processing daemon (flowd) to crash and restart. This causes a complete service outage until the system has automatically recovered. This issue affects Junos OS on MX with SPC3, and SRX Series: * 23.4 versions before 23.4R2-S7, * 24.2 versions before 24.2R2-S4, * 24.4 versions before 24.4R2-S3, * 25.2 versions before 25.2R2. This issue does not affect releases before 23.4R1.	2026-07-09	8.7

CVE-2026-57026	juniper - multiple products	An Improper Validation of Syntactic Correctness of Input vulnerability in the SIP plugin of Juniper Networks Junos OS on MX Series with SPC3 and SRX Series allows an unauthenticated, network-based attacker to cause a Denial-of-Service (DoS).If the SIP ALG is enabled on an affected device, the processing of a malformed SIP invite packet will cause a flow processing daemon (flowd) crash and restart. This leads to a complete service outage until the system has automatically recovered. This issue affects Junos OS on MX Series with SPC3 and SRX Series: * all versions before 23.2R2-S7, * 23.4 versions before 23.4R2-S8, * 24.2 versions before 24.2R2-S5, * 24.4 versions before 24.4R2-S4, * 25.2 versions before 25.2R2, * 25.4 versions before 25.4R1-S2.	2026-07-09	8.7
CVE-2026-4249	wso2 - multiple products	The throttling event handling mechanism in multiple WSO2 products accepts user-supplied JSON payloads without sufficient validation of their structure and content. This allows an unauthenticated remote attacker to inject malicious JSON data that can lead to a persistent denial of service condition. Successful exploitation of this vulnerability can disrupt the API Gateway, preventing legitimate API traffic from being processed and impacting complete service availability. The denial of service is persistent, requiring manual intervention to restore normal operations.	2026-07-06	8.6
CVE-2026-54801	siemens - multiple products	A vulnerability has been identified in CPCI85 Central Processing/Communication (All versions < V26.20), SICORE Base system (All versions < V26.20.0). The affected application contains insufficient validation of authentication credentials when processing administrative account modifications through the web API. This could allow an authenticated attacker to bypass security controls and gain unauthorized elevated privileges.	2026-07-09	8.6
CVE-2026-56690	dell - multiple products	Dell PowerFlex Manager, Version prior to 5.1.0.1, contain(s) an Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability. A low privileged attacker with remote access could potentially exploit this vulnerability, leading to Information disclosure, Information exposure, and Unauthorized access.	2026-07-10	8.5
CVE-2026-54799	siemens - multiple products	A vulnerability has been identified in CPCI85 Central Processing/Communication (All versions < V26.20), SICORE Base system (All versions < V26.20.0). The affected application contains a vulnerability in its firmware update mechanism's signature validation process. This could allow an attacker to install malicious firmware, leading to persistent code execution and system compromise.	2026-07-09	8.4
CVE-2026-15119	google - chrome	Race in GetUserMedia in Google Chrome prior to 150.0.7871.115 allowed a remote attacker who had compromised the renderer process to potentially perform a sandbox escape via a crafted HTML page. (Chromium security severity: High)	2026-07-08	8.3
CVE-2026-15120	google - chrome	Use after free in Core in Google Chrome on Windows prior to 150.0.7871.115 allowed a remote attacker who had compromised the renderer process to potentially perform a sandbox escape via a crafted HTML page. (Chromium security severity: High)	2026-07-08	8.3
CVE-2026-15122	google - chrome	Insufficient validation of untrusted input in Codecs in Google Chrome on Windows prior to 150.0.7871.115 allowed a remote attacker who had compromised the renderer process to potentially perform a sandbox escape via a crafted HTML page. (Chromium security severity: High)	2026-07-08	8.3
CVE-2026-58281	microsoft - edge_chromium	Deserialization of untrusted data in Microsoft Edge (Chromium-based) allows an unauthorized attacker to execute code over a network.	2026-07-11	8.3
CVE-2026-46591	apache - multiple products	Improper Neutralization of Special Elements in Data Query Logic vulnerability in Apache Camel Neo4J component. The camel-neo4j producer builds the Cypher WHERE clause for its match/retrieve and delete operations from the CamelNeo4jMatchProperties map. CVE-2025-66169 addressed Cypher injection through the property values by binding them as query parameters ($paramN), but the property names (the JSON keys of that map) were still concatenated into the query string verbatim in Neo4jProducer.retrieveNodes() and deleteNode(). A property name containing Cypher syntax therefore alters the structure of the executed query. Where a route maps untrusted input into the CamelNeo4jMatchProperties map - for example by passing a request body as the match map, or from a consumer that does not filter inbound Camel* headers - an attacker who controls the JSON key names can inject arbitrary Cypher and read, modify or delete any node or relationship in the Neo4j database. The CamelNeo4jMatchProperties header is itself Camel-prefixed and is filtered by the HTTP header-filter strategy, so a plain HTTP client cannot set it directly; the issue is reachable through routes that deliberately or inadvertently carry untrusted data into that header. This issue affects Apache Camel: from 4.10.0 before 4.14.8, from 4.15.0 before 4.18.3, from 4.19.0 before 4.21.0. Users are recommended to upgrade to version 4.21.0, which fixes the issue. If users are on the 4.14.x LTS releases stream, then they are suggested to upgrade to 4.14.8. If users are on the 4.18.x releases stream, then they are suggested to upgrade to 4.18.3. For deployments that cannot upgrade immediately, do not populate the CamelNeo4jMatchProperties map from untrusted input: validate or allow-list the property names (for example against ^[A-Za-z_][A-Za-z0-9_]*$) before the Neo4j producer, and ensure that any consumer feeding such a route filters inbound Camel* / camel* headers so the match header cannot be supplied by an external sender.	2026-07-06	8.2
CVE-2026-58525	microsoft - edge_chromium	Improper access control in Microsoft Edge (Chromium-based) allows an unauthorized attacker to bypass a security feature over a network.	2026-07-08	8.2

CVE-2026-33794	juniper - multiple products	An Improper Check for Unusual or Exceptional Conditions vulnerability in the advanced forwarding toolkit (evo-aftmand) of Juniper Networks Junos OS Evolved on PTX Series allows an unauthenticated network-based attacker generating continuous routing updates, resulting in unilist ECMP routes, to crash the evo-aftmand process on the PFE, leading to a Denial-of-Service (DoS). The conditions required for successful exploitation are based on a sequence of events that are outside an attacker's direct control. Unified list (unilist) ECMP routes are a specific ECMP behavior where multiple equal-cost routes share a single logical next-hop list entry. The router treats them as one route with multiple next hops and load balances traffic across that unified list. Due to an issue processing unilist ECMP routing updates, internal state corruption may occur, especially in large-scale ECMP unilist deployments, leading to the evo-aftmand process crashing, resulting in an evo-aftmand-bx core. Manual intervention is required to recover by rebooting the system or restarting the FPC. This issue affects Junos OS Evolved on PTX : * from 24.4R2-EVO before 24.4R2-S3-EVO; * from 25.2 before 25.2R2-EVO.	2026-07-09	8.2
CVE-2026-57022	juniper - multiple products	An Improper Check for Unusual or Exceptional Conditions vulnerability in the Packet Forwarding Engine (PFE) of Juniper Networks Junos OS on MX with SPC3 and SRX Series allows an unauthenticated, network-based attacker to cause a Denial-of-Service (DoS). When an affected device initiates a TCP connection to an attacker-controlled system that responds with a specific packet, this causes a PFE crash and restart, which affects all services until the system has automatically recovered. This issue can happen among others in the following scenarios: ALG, SSL proxy, UTM, RTLOG, AppQoE probing, AAMW, ICAP, URL filtering. This issue affects Junos OS on MX Series with SPC3, SRX5k Series with SPC3, SRX1600 Series, SRX2300 Series, SRX4000 Series, and vSRX Series: * all versions before 23.2R2-S4, * 23.4 versions before 23.4R2-S5, * 24.2 versions before 24.2R2.	2026-07-09	8.2
CVE-2026-57030	juniper - multiple products	A Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition') vulnerability in the packet forwarding engine (PFE) of Juniper Networks Junos OS on SRX Series allows an unauthenticated, network-based attacker to cause a Denial-of-Service (DoS). As part of the stateful traffic processing on SRX Series devices flows are being established, and removed when not needed anymore. During the removal process the timeout of a flow should be set to 3 seconds and consequentially the flow should be removed shortly after. Due to a race condition occurring when setting the timeout there is a chance (the exact conditions are outside the attackers control) that the timeout is instead set to a very high value of larger than 10,000 seconds: user@host> show security flow session | match timeout Session ID: 98784248524, Policy name: PROD-FLOW/4, HA State: Active, Timeout: 85250, Session State: Valid This will lead to an accumulation of flows which can be observed by an ever-increasing value of invalidated sessions in the output of 'show security flow session summary': user@host> show security flow session summary | match invalid Invalidated sessions: 216931These sessions can't be cleared manually with the 'clear security flow session' command, which will either lead to forwarding to stop (and the system needs to be manually recovered with a reboot) or to a flowd core and automatic reboot. This issue affects Junos OS on SRX Series: * 24.2 versions before 24.2R2-S3, * 24.4 versions before 24.4R2-S1, 24.4R2-S2, * 25.2 versions before 25.2R1-S2, 25.2R2. This issue does not affect releases earlier than 24.2R1;	2026-07-09	8.2
CVE-2026-40859	apache - multiple products	Deserialization of Untrusted Data vulnerability in Apache Camel.	2026-07-06	8.1

		The camel-vertx-http component deserializes HTTP response bodies carrying the Content-Type application/x-java-serialized-object using a raw java.io.ObjectInputStream, without applying any ObjectInputFilter (VertxHttpHelper.deserializeJavaObjectFromStream) This deserialization path is reached only when the producer endpoint is configured with transferException=true (or the component-level allowJavaSerializedObject=true) and throwExceptionOnFailure is left at its default value of true; in that case a backend HTTP response with a 5xx status and the application/x-java-serialized-object content type has its body deserialized with no class restrictions. An attacker who controls the backend the Camel producer talks to - through a man-in-the-middle position on an unencrypted (plain HTTP) connection, or by compromising the backend service - can return a crafted serialized Java object and, if a suitable gadget chain is present on the classpath, achieve remote code execution on the Camel application host. The path is not reachable in the default configuration, where transferException is false. This issue affects Apache Camel: from 4.0.0 before 4.14.8, from 4.15.0 before 4.18.3, from 4.19.0 before 4.20.0. Users are recommended to upgrade to version 4.20.0, which fixes the issue. If users are on the 4.14.x LTS releases stream, then they are suggested to upgrade to 4.14.8. If users are on the 4.18.x releases stream, then they are suggested to upgrade to 4.18.3. After upgrading, the deserialization performed by both helper utilities is constrained by a default ObjectInputFilter (allow-list java.**;javax.**;org.apache.camel.**;!*), which can be customised through the new deserializationFilter endpoint option or the JVM-wide -Djdk.serialFilter system property. For deployments that cannot upgrade immediately: do not enable transferException=true (or allowJavaSerializedObject=true) on producers that talk to untrusted or network-reachable backends; ensure producer connections use TLS (https) so that a response cannot be substituted by a man-in-the-middle; and, where the option is required, set an explicit -Djdk.serialFilter allow-list (for example java.**;org.apache.camel.**;!*) to constrain deserialization.		
CVE-2026-42527	apache - multiple products	Deserialization of Untrusted Data vulnerability in Apache Camel. The default ObjectInputFilter pattern shipped with several Apache Camel components for defense-in-depth deserialization filtering ('java.**;javax.**;org.apache.camel.**;!*', or the no-'javax.**' variant in the aggregation-repository components) uses a recursive 'java.**' glob that admits classes whose hashCode/equals/readObject methods perform network I/O, notably java.net.URL and java.net.InetAddress. When an attacker can deliver a Java-serialized payload to an affected Camel consumer, deserialization of a HashMap (or any collection that calls hashCode on its elements) containing java.net.URL keys causes the JVM to issue DNS queries to the attacker-supplied host during the deserialization side-effect. The class-level filter check passes because the resulting object's class (HashMap) is allow-listed; the DNS query is observable on an attacker-controlled DNS server, providing an out-of-band side channel. The exposure is highest on the camel-jms family because JmsBinding.extractBodyFromJms invokes ObjectMessage.getObject() unconditionally when mapJmsMessage=true (default). Affected components: camel-jms, camel-sjms, camel-amqp, camel-mina, camel-netty, camel-netty-http, camel-vertx-http, camel-infinispan, and the aggregation repository components camel-leveldb, camel-cassandraql, camel-consul, camel-sql (JDBC aggregation repository). This issue affects Apache Camel: from 4.14.0 before 4.14.8, from 4.15.0 before 4.18.3, from 4.19.0 before 4.21.0. Users are recommended to upgrade to a version that contains the CAMEL-23372 fix once available: 4.21.0 for the 4.21.x line, 4.18.3 for the 4.18.x line, and 4.14.8 for the 4.14.x line. For deployments that cannot upgrade immediately, configure a JMS-provider-side allow-list (Apache ActiveMQ Artemis 'deserializationAllowList' / 'deserializationDenyList', Apache ActiveMQ Classic 'org.apache.activemq.SERIALIZABLE_PACKAGES') as the primary mitigation, and/or override the in-code default via the endpoint-level 'deserializationFilter' option or the JVM-wide '-Djdk.serialFilter' system property with an explicit deny: '!java.net.**;java.**;javax.**;org.apache.camel.**;!*' (or '!java.net.**;java.**;org.apache.camel.**;!*' for the aggregation-repository components, which do not include javax.**).	2026-07-06	8.1
CVE-2026-43865	apache - multiple products	Deserialization of Untrusted Data vulnerability in Apache Camel Hazelcast component. The camel-hazelcast component creates and manages Hazelcast instances using a default configuration that applies no Java deserialization filter. When Camel builds the Hazelcast Config itself - that is, when no user-supplied HazelcastInstance, hazelcastConfigUri, or referenced Config bean is provided - neither Hazelcast's JavaSerializationFilterConfig nor a Camel-side ObjectInputFilter is configured, so objects received over the Hazelcast cluster protocol are deserialized inside Hazelcast's own serialization layer (ObjectInputStream.readObject) before Camel ever processes them. An attacker who can join or otherwise reach the Hazelcast cluster can publish a crafted serialized Java object that is then deserialized on every Camel node, resulting in remote code execution. The exposure is present by default and requires no opt-in endpoint configuration: any route using a hazelcast consumer (hazelcast-topic, hazelcast-queue, hazelcast-seda, hazelcast-map, hazelcast-multimap, hazelcast-replicatedmap, hazelcast-list, hazelcast-set), as well as the HazelcastAggregationRepository and HazelcastIdempotentRepository, is affected whenever the managed instance is created from Camel's default configuration. This issue affects Apache Camel: from 4.0.0 before 4.14.8, from 4.15.0 before 4.18.3, from 4.19.0 before 4.21.0. Users are recommended to upgrade to version 4.21.0, which fixes the issue. If users are on the 4.14.x LTS releases stream, then they are suggested to upgrade to 4.14.8. If users are on the 4.18.x releases stream, then they are suggested to upgrade to 4.18.3. The fix makes Camel apply a default Hazelcast JavaSerializationFilterConfig (whitelisting the java., javax. and org.apache.camel. class-name prefixes and blacklisting java.net.) to instances it creates from	2026-07-06	8.1

		its own default configuration, while leaving any user-supplied Config or HazelcastInstance untouched. For deployments that cannot upgrade immediately, configure a deserialization filter on the Hazelcast instance (Hazelcast JavaSerializationFilterConfig, or the JVM-wide system property -Djdk.serialFilter=!java.net.**;java.**;javax.**;org.apache.camel.**;!*) and enable Hazelcast cluster authentication and TLS to restrict who can reach the cluster.		
CVE-2026-49297	apache - apache-airflow-providers-google	Apache Airflow's Google provider operators `GCSToSFTPOperator` and `GCSTimeSpanFileTransformOperator` joined GCS object names returned by the bucket listing API directly to a destination filesystem path without normalisation or containment check. A user with write access to the source GCS bucket (typically a different trust principal than the DAG author — partner uploads, ingest-only service accounts, public-data buckets) could create an object whose name contains `..` segments and cause the DAG run to write the downloaded blob outside the configured destination (the SFTP `destination_path` for `GCSToSFTPOperator`; the worker-local temp directory for `GCSTimeSpanFileTransformOperator`), enabling overwrite of arbitrary files on the SFTP server or the worker host. Affects deployments that ingest from buckets writable by less-trusted principals. Users are advised to upgrade to `apache-airflow-providers-google` 22.2.1 or later.	2026-07-06	8.1
CVE-2026-3144	ibm - api_connect	IBM API Connect 12.1.0.0 through 12.1.0.3 uses default credentials which could allow an attacker to gain unauthorized access to the application before the system enforces a credential update.	2026-07-08	8.1
CVE-2026-13244	drupal - Tealium iQ Tag Management	Improperly Controlled Modification of Dynamically-Determined Object Attributes vulnerability in Drupal Tealium iQ Tag Management allows Object Injection. This issue affects Tealium iQ Tag Management versions: from 0.0.0 to 2.4.0.	2026-07-10	8.1
CVE-2026-14476	red hat - multiple products	A path traversal flaw was found in SSSD's AD GPO provider. The ad_gpo_extract_smb_components() function does not sanitize .. sequences in the gPCFileSysPath LDAP attribute, allowing an attacker with AD GPO management access to write files outside the GPO cache directory as root. On default RHEL configurations with SELinux enforcing, this can be used to inject Kerberos configuration leading to authentication bypass.	2026-07-07	8
CVE-2026-21379	qualcomm - aqt1000_firmware	Memory Corruption when allocating memory with sizes that exceed the maximum allowed value.	2026-07-06	7.8
CVE-2026-25271	qualcomm - cologne_firmware	Memory Corruption when processing asynchronous input parameters due to improper handling of modified values between check and use.	2026-07-06	7.8
CVE-2026-9165	red hat - multiple products	A flaw was found in Red Hat Advanced Cluster Security for Kubernetes (RHACS). Central does not limit the depth of GraphQL queries served on the authenticated GraphQL API. An authenticated user with a valid API token can send deeply nested queries that cause excessive resource consumption in Central, resulting in a denial of service for the management plane.	2026-07-06	7.7
CVE-2026-60002	openbsd - openssh	ssh in OpenSSH before 10.4 can have a use-after-free when a server changes its host key during a key re-exchange. (This outcome occurs only on the client side.)	2026-07-08	7.7
CVE-2026-56689	dell - multiple products	Dell PowerFlex Manager, Version prior to 5.1.0.1, contain(s) an Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability. A low privileged attacker with remote access could potentially exploit this vulnerability, leading to Information exposure.	2026-07-10	7.7
CVE-2026-24012	apache - iotdb	Uncontrolled Resource Consumption vulnerability in Apache IoTDB. Some interface fails to impose reasonable limits on the time span and aggregation interval of the query. An attacker can construct a request with extreme parameters (e.g., a very large time range combined with a minimal interval). This forces the DataNode to build an enormous result set in memory, which exhausts the Java heap and causes the DataNode process to crash. This issue affects Apache IoTDB: from 1.3.3 before 2.0.8. Users are recommended to upgrade to version 2.0.8, which fixes the issue.	2026-07-06	7.5
CVE-2026-46457	apache - multiple products	Improper Input Validation vulnerability in Apache Camel NATS component. The camel-nats component maps inbound NATS message headers into the Camel Exchange but defaulted its headerFilterStrategy to a bare new DefaultHeaderFilterStrategy() with no inbound rules configured (NatsConfiguration). With no inFilter, inFilterPattern or inFilterStartsWith set, DefaultHeaderFilterStrategy.applyFilterToExternalHeaders returns not filtered for every header name, so NatsConsumer copies every NATS message header - including Camel-internal control headers such as CamelHttpUri, CamelFileName or CamelSqlQuery - unmodified onto the Camel message. A client able to publish to the consumed NATS subject can therefore inject arbitrary Camel control headers that influence the behaviour of downstream producers in the route (for example redirecting an HTTP producer, changing a file name, or overriding a query); the injected headers also persist across internal direct, seda and vm hops. The concrete downstream impact depends on which producers the route uses. NATS message headers require NATS 2.2 or later, and the issue is reachable without credentials when the NATS server is configured without authentication (the NATS server default). This issue affects Apache Camel: from 4.0.0 before 4.14.8, from 4.15.0 before 4.18.3, from 4.19.0 before 4.21.0. Users are recommended to upgrade to version 4.21.0, which fixes the issue. If users are on the 4.14.x LTS releases stream, then they are suggested to upgrade to 4.14.8. If users are on the 4.18.x releases stream, then they are suggested to upgrade to 4.18.3. The fix makes camel-nats default to a dedicated NatsHeaderFilterStrategy that filters the Camel header namespace case-insensitively on inbound mapping, so client-supplied Camel* / camel*	2026-07-06	7.5

		headers are no longer copied into the Exchange. For deployments that cannot upgrade immediately, strip the Camel control headers from inbound NATS messages before they reach any downstream producer (for example removeHeaders('Camel*') and removeHeaders('camel*') at the start of the route), and enable authentication on the NATS server so that only trusted clients can publish to the consumed subject.		
CVE-2026-46585	apache - multiple products	Improper Input Validation, Authorization Bypass Through User-Controlled Key vulnerability in Apache Camel Lucene Component. The camel-lucene producer reads the search phrase from an Exchange header (LuceneConstants.HEADER_QUERY) whose value was the plain string QUERY (and RETURN_LUCENE_DOCS for HEADER_RETURN_LUCENE_DOCS). Because these names do not start with the Camel / camel prefix, HttpHeaderFilterStrategy - which blocks only the Camel header namespace on the HTTP boundary - let them pass from an inbound HTTP request straight into the Exchange. In a route that exposes a Lucene query operation behind an HTTP consumer (for example platform-http), any HTTP client could therefore set the QUERY header and have its value executed against the full-text index, overriding the query the route intended to run. Depending on what is indexed, this allows reading documents the request should not have access to (for example a match-all query returns the entire index, or the route's intended per-user filter can be replaced), and expensive regular-expression queries can consume significant CPU. No credentials are required when the HTTP consumer is unauthenticated. This issue affects Apache Camel: from 4.0.0 before 4.14.8, from 4.15.0 before 4.18.3, from 4.19.0 before 4.21.0. Users are recommended to upgrade to version 4.21.0, which fixes the issue. If users are on the 4.14.x LTS releases stream, then they are suggested to upgrade to 4.14.8. If users are on the 4.18.x releases stream, then they are suggested to upgrade to 4.18.3. After upgrading, routes that set the query via the raw header name must use CamelLuceneQuery (and CamelLuceneReturnLuceneDocs) instead of QUERY / RETURN_LUCENE_DOCS. For deployments that cannot upgrade immediately, strip the attacker-controllable headers before the Lucene producer and set the query from a trusted source (for example removeHeader('QUERY') and removeHeader('RETURN_LUCENE_DOCS'), then setHeader('QUERY', constant(...)) at the start of the route).	2026-07-06	7.5
CVE-2026-46592	apache - multiple products	Improper Input Validation, Unintended Proxy or Intermediary ('Confused Deputy') vulnerability in Apache Camel CXF SOAP component. The camel-cxf producer selects which SOAP operation to invoke on the backend service from the operationName (and operationNamespace) Exchange header, whose constant values (CxfConstants.OPERATION_NAME / OPERATION_NAMESPACE) were the plain strings operationName / operationNamespace. Because these names do not start with the Camel / camel prefix, HttpHeaderFilterStrategy - which blocks only the Camel header namespace on the HTTP boundary - let them pass from an inbound HTTP request straight into the Exchange. In a route that bridges an HTTP consumer (for example platform-http) into a cxf: producer, any HTTP client could therefore set the operationName header and have CxfProducer resolve and invoke a different WSDL operation than the route intended - for example replacing a read operation with a destructive one - against the backend SOAP service (a confused-deputy redirection). The constant is defined in the shared camel-cxf-common module, so the same non-prefixed names also applied to camel-cxfrs. No credentials are required when the bridging consumer is unauthenticated. This issue affects Apache Camel: from 4.0.0 before 4.14.8, from 4.15.0 before 4.18.3, from 4.19.0 before 4.21.0. Users are recommended to upgrade to version 4.21.0, which fixes the issue. If users are on the 4.14.x LTS releases stream, then they are suggested to upgrade to 4.14.8. If users are on the 4.18.x releases stream, then they are suggested to upgrade to 4.18.3. After upgrading, the operation-selection headers are named CamelCxfOperationName / CamelCxfOperationNamespace and are filtered at transport boundaries; see the 4.21 upgrade guide for the cross-transport carrier-header pattern. For deployments that cannot upgrade immediately, do not select the CXF operation from untrusted input: strip the operationName and operationNamespace headers from any untrusted ingress before the cxf: producer and set the operation from a trusted source in the route.	2026-07-06	7.5
CVE-2026-46726	apache - multiple products	Improper Input Validation, Exposure of Sensitive Information to an Unauthorized Actor, Server-Side Request Forgery (SSRF) vulnerability in Apache Camel in Vertx Websocket component. The camel-vertx-websocket consumer mapped inbound WebSocket query and path parameters into the Camel Exchange header map without applying any HeaderFilterStrategy (VertxWebsocketConsumer.populateExchangeHeaders()). Because nothing blocked the Camel header namespace, a client connecting to the WebSocket endpoint could set Camel-internal control headers - including CamelHttpUri (Exchange.HTTP_URI) - simply by supplying them as query parameters. In a route where the WebSocket consumer feeds a downstream HTTP producer, the injected CamelHttpUri redirects the server-side HTTP request to an attacker-chosen destination (server-side request forgery - for example to an internal service or a cloud metadata endpoint). In addition, the HTTP producer resolves Camel property placeholders on the resulting (attacker-controlled) URI, so placeholders embedded in the injected value - such as an environment-variable reference, an application property, or a vault reference - are resolved to their real values and sent to the attacker, disclosing environment variables, application properties and vault secrets. When the WebSocket endpoint is exposed without authentication, this is reachable by an unauthenticated remote attacker. This issue affects Apache Camel: from 4.0.0 before 4.14.8, from 4.15.0 before 4.18.3, from 4.19.0 before 4.21.0.	2026-07-06	7.5

		Users are recommended to upgrade to version 4.21.0, which fixes the issue. If users are on the 4.14.x LTS releases stream, then they are suggested to upgrade to 4.14.8. If users are on the 4.18.x releases stream, then they are suggested to upgrade to 4.18.3. The fix makes the affected consumers apply a HeaderFilterStrategy that filters the Camel header namespace case-insensitively on inbound mapping, so externally-supplied Camel* / camel* headers are no longer copied into the Exchange. For deployments that cannot upgrade immediately, strip the Camel control headers from the inbound message before they reach any downstream producer (for example removeHeaders('Camel*') and removeHeaders('camel*') at the start of the route), require authentication on the WebSocket endpoint, and avoid bridging an untrusted consumer directly into an HTTP producer whose target URI can be driven from message headers.		
CVE-2026-55993	apache - multiple products	Improper Input Validation, Exposure of Sensitive Information to an Unauthorized Actor, Server-Side Request Forgery (SSRF) vulnerability in Apache Camel in Atmosphere Websocket Component. The camel-atmosphere-websocket consumer mapped inbound WebSocket query parameters into the Camel Exchange header map without applying any HeaderFilterStrategy (WebsocketConsumer.sendEventNotification() iterates the query-string map collected in WebsocketConsumer.service() and copies each entry into the Exchange). Because nothing blocked the Camel header namespace, a client connecting to the WebSocket endpoint could set Camel-internal control headers - including CamelHttpUri (Exchange.HTTP_URI) - simply by supplying them as query parameters. In a route where the WebSocket consumer feeds a downstream HTTP producer, the injected CamelHttpUri redirects the server-side HTTP request to an attacker-chosen destination (server-side request forgery - for example to an internal service or a cloud metadata endpoint). In addition, the HTTP producer resolves Camel property placeholders on the resulting (attacker-controlled) URI, so placeholders embedded in the injected value - such as an environment-variable reference, an application property, or a vault reference - are resolved to their real values and sent to the attacker, disclosing environment variables, application properties and vault secrets. When the WebSocket endpoint is exposed without authentication, this is reachable by an unauthenticated remote attacker. This issue affects Apache Camel: from 4.0.0 before 4.14.8, from 4.15.0 before 4.18.3, from 4.19.0 before 4.21.0. Users are recommended to upgrade to version 4.21.0, which fixes the issue. If users are on the 4.14.x LTS releases stream, then they are suggested to upgrade to 4.14.8. If users are on the 4.18.x releases stream, then they are suggested to upgrade to 4.18.3. The fix makes the consumer apply the HeaderFilterStrategy it already inherits from the HTTP/servlet stack, filtering the Camel header namespace case-insensitively on inbound mapping, so externally-supplied Camel* / camel* headers are no longer copied into the Exchange. For deployments that cannot upgrade immediately, strip the Camel control headers from the inbound message before they reach any downstream producer (for example removeHeaders('Camel*') and removeHeaders('camel*') at the start of the route), require authentication on the WebSocket endpoint, and avoid bridging an untrusted consumer directly into an HTTP producer whose target URI can be driven from message headers.	2026-07-06	7.5
CVE-2026-55994	apache - multiple products	Improper Input Validation, Exposure of Sensitive Information to an Unauthorized Actor, Server-Side Request Forgery (SSRF) vulnerability in Apache Camel in Iggy component. The camel-iggy consumer mapped the user-headers of inbound Iggy messages into the Camel Exchange header map without applying any HeaderFilterStrategy (IggyFetchRecords copied the message user-headers straight into the Exchange). Because nothing blocked the Camel header namespace, an actor able to publish to the consumed Iggy stream/topic could set Camel-internal control headers - including CamelHttpUri (Exchange.HTTP_URI) - simply by supplying them as message user-headers. In a route where the Iggy consumer feeds a downstream HTTP producer, the injected CamelHttpUri redirects the server-side HTTP request to an attacker-chosen destination (server-side request forgery - for example to an internal service or a cloud metadata endpoint). In addition, the HTTP producer resolves Camel property placeholders on the resulting (attacker-controlled) URI, so placeholders embedded in the injected value - such as an environment-variable reference, an application property, or a vault reference - are resolved to their real values and sent to the attacker, disclosing environment variables, application properties and vault secrets. This issue affects Apache Camel: from 4.17.0 before 4.18.3, from 4.19.0 before 4.21.0. Users are recommended to upgrade to version 4.21.0, which fixes the issue. If users are on the 4.18.x releases stream, then they are suggested to upgrade to 4.18.3. The fix adds a dedicated IggyHeaderFilterStrategy (and a headerFilterStrategy endpoint option) that filters the Camel header namespace case-insensitively on inbound mapping, so externally-supplied Camel* / camel* headers are no longer copied into the Exchange. For deployments that cannot upgrade immediately, strip the Camel control headers from the inbound message before they reach any downstream producer (for example removeHeaders('Camel*') and removeHeaders('camel*') at the start of the route), restrict who can publish to the consumed Iggy stream/topic, and avoid bridging an untrusted consumer directly into an HTTP producer whose target URI can be driven from message headers.	2026-07-06	7.5
CVE-2026-53482	dell - multiple products	Dell PowerProtect Data Domain, versions 7.7.1.0 through 8.7, LTS2026 release version 8.6.1.0 through 8.6.1.10, LTS2025 release version 8.3.1.0 through 8.3.1.30, LTS2024 release versions 7.13.1.0 through 7.13.1.70 contain an Integer overflow or wraparound vulnerability. An unauthenticated attacker with remote access could potentially exploit this vulnerability, leading to denial of service.	2026-07-08	7.5
CVE-2026-15111	google - chrome	Use after free in Views in Google Chrome prior to 150.0.7871.115 allowed a remote attacker who convinced a user to engage in specific UI gestures to potentially exploit heap corruption via a crafted HTML page. (Chromium security severity: High)	2026-07-08	7.5

CVE-2026-15117	google - chrome	Use after free in Payments in Google Chrome prior to 150.0.7871.115 allowed a remote attacker who convinced a user to engage in specific UI gestures to potentially exploit heap corruption via a crafted HTML page. (Chromium security severity: High)	2026-07-08	7.5
CVE-2026-57111	apache - helix	Permissive Cross-Origin Resource Sharing (CORS) in the REST API (helix-rest, org.apache.helix.rest.server.filters.CORSFilter) in Apache Helix through 2.0.0 on all platforms allows a remote attacker controlling a web page visited by an authorized user to read responses from and issue cross-origin requests to administrative REST endpoints via a cross-origin request from an arbitrary origin, since the filter unconditionally returns Access-Control-Allow-Origin: * together with Access-Control-Allow-Credentials: true and reflects arbitrary Access-Control-Request-Method / Access-Control-Request-Headers values in preflight responses. Users are recommended to upgrade to version 2.0.1, which fixes this issue.	2026-07-09	7.5
CVE-2026-59692	red hat - multiple products	A stack buffer overflow vulnerability was found in GStreamer's DTLS plugin. During a DTLS handshake, the peer certificate Subject Distinguished Name is printed into a fixed-size 2048-byte stack buffer without bounds checking. A remote unauthenticated attacker can send a certificate with an oversized Subject DN that exceeds the buffer, causing a stack buffer overflow and process crash, resulting in denial of service.	2026-07-09	7.5
CVE-2026-40006	apache software foundation - Apache IoTDB	Memory Allocation with Excessive Size Value, Allocation of Resources Without Limits or Throttling, Missing Authentication for Critical Function vulnerability in Apache IoTDB. When pipe_air_gap_receiver_enabled=true, the IoTDB AirGap pipe receiver accepts raw TCP connections on port 9780 with no authentication. The readLength method reads an attacker-controlled 32-bit integer from the socket and readData passes it directly to new byte[length] with no upper-bound check. An unauthenticated attacker can cause the JVM to attempt an allocation of up to 2,147,483,647 bytes per connection, exhausting heap memory and crashing or severely degrading the DataNode process. This issue affects Apache IoTDB: from 1.0.0 before 2.0.10. Users are recommended to upgrade to version 2.0.10, which fixes the issue.	2026-07-10	7.5
CVE-2026-40007	apache software foundation - Apache IoTDB	Uncontrolled Recursion, Uncontrolled Resource Consumption vulnerability in Apache IoTDB. When pipe_air_gap_receiver_enabled=true, the IoTDB AirGap receiver's readLength method calls itself recursively each time it recognises the E-language prefix in socket data, with no depth limit. An unauthenticated attacker can send a stream of repeated E-language prefixes that drives the recursion arbitrarily deep, exhausting the receiver thread's JVM stack and raising StackOverflowError. This issue affects Apache IoTDB: from 1.0.0 before 2.0.10. Users are recommended to upgrade to version 2.0.10, which fixes the issue.	2026-07-10	7.5
CVE-2026-40452	apache software foundation - Apache IoTDB	Incorrect Authorization, Improper Access Control vulnerability in Apache IoTDB. Authorization bypass in /rest/v2/fastLastQuery exposes last-value data to unauthorized authenticated users. This issue affects Apache IoTDB: from 1.3.5 before 1.3.8, from 2.0.5 before 2.0.10. Users are recommended to upgrade to version 2.0.10, which fixes the issue.	2026-07-10	7.5
CVE-2026-40454	apache software foundation - Apache IoTDB C++ client	Out-of-bounds Read, Improper Input Validation vulnerability in Apache IoTDB C++ client. Out-of-bounds reads in IoTDB C++ client TsBlock deserializer crash client process on malformed server data. This issue affects Apache IoTDB C++ client: from 1.3.5 before 1.3.8, from 2.0.5 before 2.0.10. Users are recommended to upgrade to version 2.0.10, which fixes the issue.	2026-07-10	7.5
CVE-2026-33382	grafana - multiple products	Several Grafana API endpoints, some of them unauthenticated, do not limit the size of the request body before processing it. An attacker can send very large payloads that force excessive memory allocation, potentially exhausting memory and causing a denial of service.	2026-07-10	7.5
CVE-2026-15081	drupal - Location Selector	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in Drupal Location Selector allows SQL Injection. This issue affects Location Selector versions: from 0.0.0 to 1.3.0.	2026-07-10	7.4
CVE-2026-43866	apache - multiple products	Deserialization of Untrusted Data vulnerability in Apache Camel, Apache Camel JMS component. JmsBinding.extractBodyFromJms() in camel-jms - and the equivalent JmsBinding in camel-sjms - deserializes the payload of an incoming JMS ObjectMessage via jakarta.jms.ObjectMessage.getObject() whenever the mapJmsMessage option is enabled (the default) and Camel acts as a JMS consumer. The CVE-2026-40860 hardening added a post-deserialization class check that rejects classes outside the default allow-list java.**;javax.**;org.apache.camel.**;!*. However org.apache.camel.support.DefaultExchangeHolder itself lives in the allow-listed org.apache.camel.** namespace, so an ObjectMessage whose top-level object is a DefaultExchangeHolder passes the check. The receiving side then calls DefaultExchangeHolder.unmarshal() on it without requiring the transferExchange option to be enabled - an asymmetric trust boundary, since the sending side gates ObjectMessage and transferExchange handling but the receiving side did not - writing every non-null field of the holder into the Exchange: the message body, the IN and OUT headers, the exchange properties, the variables, the exchange id and the exception. An attacker who can publish an	2026-07-06	7.3

		ObjectMessage to a queue or topic consumed by an affected Camel application can therefore inject arbitrary Exchange state using only universally-trusted java.lang and java.util types, with no deserialization gadget chain required, to manipulate routing and headers, exchange properties and error handling. The same handling applies to camel-sjms and camel-sjms2, and to the JMS-family components built on JmsComponent and JmsBinding: camel-amqp, camel-activemq and camel-activemq6. This is a bypass of the CVE-2026-40860 fix rather than a flaw in it. This issue affects Apache Camel: from 3.0.0 before 4.14.8, from 4.15.0 before 4.18.3, from 4.19.0 before 4.21.0; Apache Camel: from 3.0.0 before 4.14.8, from 4.15.0 before 4.18.3, from 4.19.0 before 4.21.0. Users are recommended to upgrade to version 4.21.0, which fixes the issue. If users are on the 4.14.x LTS releases stream, then they are suggested to upgrade to 4.14.8. If users are on the 4.18.x releases stream, then they are suggested to upgrade to 4.18.3. After upgrading, JMS ObjectMessage handling is disabled by default in camel-jms, camel-sjms and the JMS-family components (a new objectMessageEnabled option defaults to false at the component and endpoint level), so an incoming ObjectMessage - including a DefaultExchangeHolder payload - is no longer deserialized unless the option is explicitly enabled; only set objectMessageEnabled=true when the consumed JMS destination is fed exclusively by trusted producers. For deployments that cannot upgrade immediately, restrict publish access to the queues and topics consumed by Camel to trusted producers via JMS broker authorization, and do not expose JMS consumers that map ObjectMessage bodies to untrusted networks; a JMS-provider deserialization allow-list does not mitigate this specific bypass because the crafted payload uses only universally-trusted classes.		
CVE-2026-46587	apache - multiple products	Improper Input Validation vulnerability in Apache Camel. This issue affects Apache Camel: through 4.14.7, from 4.15.0 through 4.18.2, from 4.19.0 through 4.20.0. Users are recommended to upgrade to version 4.14.8, 4.18.3, 4.21.0, which fixes the issue.	2026-07-06	7.3
CVE-2026-46588	apache - multiple products	Improper Input Validation vulnerability in Apache Camel. This issue affects Apache Camel: through 4.14.7, from 4.15.0 through 4.18.2, from 4.19.0 through 4.20.0. Users are recommended to upgrade to version 4.14.8, 4.18.3, 4.21.0, which fixes the issue.	2026-07-06	7.3
CVE-2026-49042	apache - multiple products	Improper Input Validation vulnerability in Apache Camel. This issue affects Apache Camel: from 4.8.0 through 4.18.2, from 4.19.0 through 4.20.0. Users are recommended to upgrade to version 4.18.3, 4.21.0, which fixes the issue.	2026-07-06	7.3
CVE-2026-43825	apache - multiple products	Untrusted Java Deserialization in Apache OpenNLP SvmDoccatModel Versions Affected: before 3.0.0-M4 (libsvm document categorization module; introduced in OPENNLP-1808 and only present on the 3.x line) Description: SvmDoccatModel.deserialize(InputStream) reads an attacker-controlled stream with java.io.ObjectInputStream and calls readObject() without an ObjectInputFilter installed. ObjectInputStream materialises every class referenced in the stream before the resulting object is cast to SvmDoccatModel, so the cast that follows readObject() executes only after the foreign object graph has already been deserialised in full. If a Java deserialization gadget chain is available on the consumer's classpath, a crafted payload supplied to deserialize() executes arbitrary code in the JVM that loads it. Apache OpenNLP itself does not ship a known gadget chain, so the realistic risk is to downstream applications that embed the libsvm module alongside vulnerable transitive dependencies. The method is public and static, so any caller can pass an untrusted stream to it directly. The practical impact is remote code execution against processes that load SvmDoccatModel instances from untrusted or semi-trusted origins. Mitigation: 3.x users should upgrade to 3.0.0-M4. Users who cannot upgrade immediately should treat all serialized SvmDoccatModel streams as untrusted input unless their provenance is verified, and should avoid invoking SvmDoccatModel.deserialize() on streams supplied by end users or fetched from third-party sources without integrity checks.	2026-07-06	7.3
CVE-2026-53479	dell - multiple products	Dell PowerProtect Data Domain, versions 7.7.1.0 through 8.7, LTS2026 release version 8.6.1.0 through 8.6.1.10, LTS2025 release version 8.3.1.0 through 8.3.1.30, LTS2024 release versions 7.13.1.0 through 7.13.1.70 contain an improper neutralization of special elements used in an OS command ('OS command Injection') vulnerability. A remote high privileged attacker could potentially exploit this vulnerability, leading to protection mechanism bypass. This is a Critical	2026-07-07	7.2

		vulnerability as it allows an attacker to invoke arbitrary command execution with root privileges; so Dell recommends customers to upgrade at the earliest opportunity.		
CVE-2026-24697	cisco - rv130_firmware	An OS command injection vulnerability exists in the start_bonjour() function of the "rc" binary in Cisco RV130/RV130W with firmware 1.0.3.55 and RV110W routers with firmware 1.2.2.5 / 1.2.2.8. The wan_hostname configuration parameter is not properly sanitized, which could allow an authenticated remote attacker to execute arbitrary OS commands with root privileges.	2026-07-08	7.2
CVE-2026-24698	cisco - rv130_firmware	An OS command injection vulnerability exists in the save_syslog_to_file() function of the "httpd" binary in Cisco RV130/RV130W with firmware 1.0.3.55 and RV110W routers with firmware 1.2.2.5 / 1.2.2.8. The model_name configuration parameter is not properly sanitized, which could allow an authenticated remote attacker to execute arbitrary OS commands with root privileges.	2026-07-08	7.2
CVE-2026-24699	cisco - rv130_firmware	An OS command injection vulnerability exists in the sub_34984() function of the "rc" binary in Cisco RV130/RV130W with firmware 1.0.3.55 and RV110W routers with firmware 1.2.2.5 / 1.2.2.8. The lan_ipv6_prefixlen configuration parameter is not properly sanitized, which could allow an authenticated remote attacker to execute arbitrary OS commands with root privileges.	2026-07-08	7.2
CVE-2026-24700	cisco - rv130_firmware	An OS command injection vulnerability exists in the start_lltd() function of the "rc" binary in Cisco RV130/RV130W with firmware 1.0.3.55 and RV110W routers with firmware 1.2.2.5 / 1.2.2.8. The machine_name configuration parameter is not properly sanitized, which could allow an authenticated remote attacker to execute arbitrary OS commands with root privileges.	2026-07-08	7.2
CVE-2026-0288	paloaltonetworks - multiple products	Multiple buffer overflow vulnerabilities in the User-ID Terminal Server Agent (TSA) component of Palo Alto Networks PAN-OS software allow an unauthenticated attacker with network access to cause a denial of service (DoS) condition or potentially execute arbitrary code by sending specially crafted network traffic. The security risk posed by this issue is minimized when the User-ID Terminal Server Agent connectivity is restricted to only trusted internal IP addresses according to our recommended best practice deployment guidelines https://docs.paloaltonetworks.com/ngfw/help/10-2/user-identification/device-user-identification-terminal-services-agents#:~:text=To%20minimize%20security%20risk%2C%20restrict%20TS%20Agent%20connectivity%20to%20trusted%20internal%20IP%20addresses%20only. . Panorama is not impacted by this vulnerability.	2026-07-08	7.2
CVE-2026-21383	qualcomm - fastconnect_6900_firmware	Cryptographic Issue when using a static initialization vector for AES-GCM key wrapping, which requires a unique value for each call to ensure security.	2026-07-06	7.1
CVE-2026-41122	dell - multiple products	Dell PowerProtect Data Domain, versions 7.7.1.0 through 8.7, LTS2026 release version 8.6.1.0 through 8.6.1.10, LTS2025 release version 8.3.1.0 through 8.3.1.30, LTS2024 release versions 7.13.1.0 through 7.13.1.70 contain a stored cross-site scripting vulnerability. An unauthenticated attacker with remote access could potentially exploit this vulnerability. Exploitation may lead to information disclosure, session theft, or client-side request forgery.	2026-07-08	7.1
CVE-2026-59691	red hat - multiple products	A heap buffer overflow vulnerability was found in GStreamer's rfbsrc plugin. When a client connects to a malicious RFB/VNC server that advertises a 16bpp framebuffer and sends Hextile-encoded updates, the Hextile background fill path writes 32-bit pixel values into a buffer allocated for 16-bit pixels. This type mismatch causes an out-of-bounds heap write that can lead to denial of service (process crash) and potential memory corruption.	2026-07-09	7.1
CVE-2026-54798	siemens - multiple products	A vulnerability has been identified in CPCI85 Central Processing/Communication (All versions < V26.20), SICORE Base system (All versions < V26.20.0). The affected application includes a debugging interface that is accessible through HTTP endpoints. This could allow an authenticated attacker to disrupt the system by crashing the web process causing denial of service conditions.	2026-07-09	7.1
CVE-2026-33801	juniper - multiple products	An Improper Check for Unusual or Exceptional Conditions vulnerability in the routing protocol daemon (RPD) of Juniper Networks Junos OS and Junos OS Evolved allows an adjacent, unauthenticated attacker sending a specific BGP update over an established BGP session to cause a Denial-of-Service (DoS). Upon receipt of a specifically malformed non-inet/inet6 unicast BGP update, an RPD crash and restart is triggered, which will cause a complete service outage until routing has reconverged. The rpd crash occurs before the update can be readvertised, so there is no downstream propagation. This issue affects: * Junos OS versions 25.2 before 25.2R2; * Junos OS Evolved versions 25.2 before 25.2R2-EVO. This issue doesn't affect Junos OS versions before 25.2R1 nor Junos OS Evolved versions before 25.2R1-EVO.	2026-07-09	7.1
CVE-2026-57019	juniper - multiple products	An Improper Validation of Specified Quantity in Input vulnerability in the Packet Forwarding Engine (pfe) of Juniper Networks Junos OS on MX Series allows an unauthenticated, adjacent attacker to cause a Denial-of-Service (DoS).	2026-07-09	7.1

		When a specific packet is received from device in the same broadcast domain, an affected system calculates the packet size incorrectly. This causes further packet processing to fail, which triggers an FPC major error, resulting in a FPC reset impacting traffic until the FPC has automatically recovered. Affected scenarios are: MAP-T, or non-IP traffic encapsulated in IP (e.g. MPLS over GRE). When this issue happens the following logs can be observed: fpc<#> CMError: /fpc/0/pfe/0/cm/0/MQSS(0)/0/MQSS_CMERROR_LI_INT_REG_UNROLL_TAIL_LENGTH_OVF (0x2205eb), scope: pfe, category: functional, severity: major, module: MQSS(0), type: LI: Unroll TAIL length overflow, oc_category: default fpc<#> Performing action reset-fru for error /fpc/0/pfe/0/cm/0/MQSS(0)/0/MQSS_CMERROR_LI_INT_REG_UNROLL_TAIL_LENGTH_OVF (0x2205eb) in module: MQSS(0) with scope: pfe category: functional level: major, oc_category: default This issue affects Junos OS on MX Series: * all versions before 23.2R2-S6, * 23.4 versions before 23.4R2-S7, * 24.2 versions before 24.2R2-S4, * 24.4 versions before 24.4R2-S4, * 25.2 versions before 25.2R2.		
CVE-2026-57020	juniper - multiple products	An Improper Check for Unusual or Exceptional Conditions vulnerability in the packet forwarding engine (pfe) of Juniper Networks Junos OS on QFX10000 Series allows an unauthenticated, adjacent attacker to cause a Denial-of-Service (DoS). On all QFX10000 platforms in an EVPN-VxLAN scenario, if an attacker sends IPv6 multicast traffic and these packets reach the non-IRB interface of a spine switch it floods the packet to other spines and all Ethernet Segment Identifier (ESI) leaf switches. This flooding causes the packet to be forwarded in a endless loop, which can lead to saturation of the involved links and in turn impact to legitimate traffic. This issue affects Junos OS on QFX10000 Series: * all versions before 23.2R2-S7, * 23.4 versions before 23.4R2-S8, * 24.2 versions before 24.2R2-S4, * 24.4 versions before 24.4R2-S4. This issue does not affect Junos version after 24.4 as the QFX10000 Series devices are not supported on newer versions anymore.	2026-07-09	7.1
CVE-2026-57027	juniper - multiple products	A Missing Release of Memory after Effective Lifetime vulnerability in the packet forwarding engine (pfe) of Juniper Networks Junos OS on specific EX Series devices allows an unauthenticated adjacent attacker to cause a Denial-of-Service (DoS).When sFlow is configured in a Virtual Chassis (VC) scenario with EX4100 Series or EX4400 Series devices, multicast traffic which is received on one VC member and sent out on another member leads to a memory leak and ultimately an FPC crash and restart. The leak can be monitored by watching the continuous increase of the buffer values in the output of: user@host> show chassis fpc This issue affects Junos OS on EX4100 Series and EX4400: * all versions before 23.2R2-S7, * 23.4 versions before 23.4R2-S7, * 24.2 versions before 24.2R2-S4, * 24.4 versions before 24.4R2.	2026-07-09	7.1
CVE-2026-57032	juniper - multiple products	An Improper Handling of Undefined Parameters vulnerability in the packet forwarding engine (pfe) of Juniper Networks Junos OS on EX Series devices allows an authenticated attacker with low privileges to cause a Denial-of-Service (DoS). If an attempt is made to subscribe to an unsupported telemetry sensor path on EX2300, EX3400, EX4000, EX4100 and EX4400 via gRPC, this causes the FPC to crash. This leads to a complete service outage until the module has automatically restarted.	2026-07-09	7.1

		The following log message can be seen when this issue happens: agentd[<PID>]: AGENTD_RESOURCE_NOT_FOUND: No resource name found for <sensor> This issue affects Junos OS on EX2300, EX3400, EX4000, EX4100 and EX4400 devices: * all versions before 23.2R2-S7, * 23.4 versions before 23.4R2-S8, * 24.2 versions before 24.2R2-S5, * 24.4 versions before 24.4R2.		
CVE-2026-58470	gnu - wget	GNU Wget through 1.25.0, fixed in commit 43d3ba9, contains an integer overflow vulnerability in the parse_content_range() function within src/http.c that allows server-controlled values to cause signed integer arithmetic to overflow. Attackers can supply malicious Content-Range header values to trigger undefined behavior and download desynchronization in the affected client.	2026-07-07	6.9
CVE-2026-33803	juniper - multiple products	An Improper Restriction of Communication Channel to Intended Endpoints vulnerability in Juniper Networks Junos OS Evolved allows an unauthenticated, network-based attacker to cause a limited information disclosure and availability impact to the device. Due to a wrong initialization, a process which should only be able to communicate internally within the device can be reached over the network via an open port. This leads to a device being inadvertently exposed and increased CPU cycles spent processing ingress packets. This issue affects Junos OS Evolved: * all versions before 23.2R2-S7-EVO, * 23.4 versions before 23.4R2-S8-EVO, * 24.2 versions before 24.2R2-S5-EVO, * 24.4 versions before 24.4R2-S4-EVO, * 25.2 versions before 25.2R2-S1-EVO, * 25.4 versions before 25.4R1-S2-EVO.	2026-07-09	6.9
CVE-2026-57021	juniper - multiple products	An Out-of-bounds Write vulnerability in the http-gatekeeper (http-gk) of Juniper Networks Junos OS on SRX Series allows an unauthenticated, network-based attacker to cause a Denial-of-Service (DoS). If an SRX Series device is configured for remote-access VPN with pre-logon compliance check, a network-based attacker sending specifically formatted requests can trigger an out of bounds write leading to an http-gk process crash. This crash leads to unavailability of all services depending on the [system services web-management] configuration (like J-Web, remote access VPN and firewall authentication) until the process automatically restarts. This issue affects Junos OS on SRX Series: * 23.2 versions before 23.2R2-S7, * 23.4 versions before 23.4R2-S8, * 24.2 versions before 24.2R2-S4, * 24.4 versions before 24.4R2-S4, * 25.2 versions before 25.2R2, * 25.4 versions before 25.4R1-S1, 25.4R2.	2026-07-09	6.9
CVE-2026-57024	juniper - multiple products	A Use of Multiple Resources with Duplicate Identifier vulnerability in the IKE daemon (iked) of Juniper Networks Junos OS on MX with SPC3 and SRX Series allows an unauthenticated, network-based attacker to cause a Denial-of-Service (DoS). On an MX with SPC3 and SRX devices configured for VPN service, when a large number of VPN negotiations fail a peer index rollover will eventually occur. As a result, new peers are assigned index values that are already in use and the iked process starts to crash repeatedly. This results in failure to establish new VPN connections and rekeying existing ones. To restore service the system must be rebooted. Please note that the index value can't be monitored, so customers should monitor tunnel up and down events and if a lot of events occur over an extended period of time it becomes likely that this issue occurs. To be exposed to this issue the system needs to run iked (vs. kmd which is not affected), which can be verified with: user@host> show system processes extensive | match "KMD|IKED" This issue affects Junos OS on MX with SPC3, SRX Series: * all versions before 23.2R2-S7,	2026-07-09	6.9

		* 23.4 versions before 23.4R2-S6, * 24.2 versions before 24.2R2-S3, * 24.4 versions before 24.4R2-S4, * 25.2 versions before 25.2R1-S1.		
CVE-2026-57028	juniper - multiple products	An Improper Restriction of Communication Channel to Intended Endpoints vulnerability in Juniper Networks Junos OS Evolved allows an unauthenticated, network-based attacker to cause license exhaustion. Due to an incorrect initialization, a process which should only be able to communicate internally within the device, can be reached over the network via an open port. This leads to unauthorized access to the license management. This issue affects all Junos OS Evolved versions before 23.2R2-EVO.	2026-07-09	6.9
CVE-2026-57054	juniper - multiple products	A Use of Incorrectly-Resolved Name or Reference vulnerability in the URL filtering plugin of Juniper Networks Junos OS on MX Series allows an unauthenticated, network-based attacker to bypass web filtering and access downstream resources that should be unreachable. If an MX Series device is configured with web filtering, and an attacker sends a request with a specifically formatted URL, this request will get forwarded despite the system being configured to block it. In turn, an attacker can access downstream resources that are expected to be unreachable. This issue affects Junos OS on MX Series: * all versions before 23.2R2-S7, * 23.4 versions before 23.4R2-S8, * 24.2 versions before 24.2R2-S5, * 24.4 versions before 24.4R2-S4, * 25.2 versions before 25.2R1-S1, * 25.4 versions before 25.4R1-S2, 25.4R2.	2026-07-09	6.9
CVE-2026-33802	juniper - multiple products	A Missing Authorization vulnerability in the CLI of Juniper Networks Junos OS on EX Series allows a local, authenticated attacker to cause a Denial-of-Service (DoS). On EX2300, EX4000, EX4100, EX4300-MP (Multigigabit) and EX4400 switches, an authenticated, local attacker with no specific permissions or class can execute a specific, privileged CLI 'request' command which will cause complete traffic impact until the system automatically recovers. This issue affects Junos OS on EX2300, EX4000, EX4100, EX4300-MP (Multigigabit) and EX4400: * 23.2R2 versions before 23.2R2-S6, * 23.4 versions before 23.4R2-S8, * 24.2 versions before 24.2R2-S4, * 24.4 versions before 24.4R2-S3, * 25.2 versions before 25.2R2, * 25.4 versions before 25.4R1-S1.	2026-07-09	6.8
CVE-2026-57025	juniper - multiple products	A Return of Pointer Value Outside of Expected Range vulnerability in the fileio library of Juniper Networks Junos OS and Junos OS Evolved allows a local, low-privilged attacker to cause a Denial-of-Service (DoS). On EX Series, QFX Series and MX Series a low-privileged attacker issuing a specific 'show l2-learning' or 'show ethernet-switching' command will cause an l2ald crash which will lead to a temporary service impact for all layer 2 services until the process has automatically restarted. This issue affects EX Series, QFX Series, MX Series: Junos OS: * all versions before 23.2R2-S7, * 23.4 versions before 23.4R2-S7, * 24.2 versions before 24.2R2, * 24.4 versions before 24.4R1-S2. Junos OS Evolved: * all versions before 23.2R2-S7-EVO, * 23.4 versions before 23.4R2-S8-EVO, * 24.2 versions before 24.2R2-EVO, * 24.4 versions before 24.4R1-S3-EVO.	2026-07-09	6.8

CVE-2026-8595	grafana - multiple products	A user with Editor permissions can craft a dashboard whose table (TableNG) panel contains a malicious field name that executes as a script in the browser of any user who views the dashboard (stored cross-site scripting).	2026-07-10	6.8
CVE-2025-59615	qualcomm - fastconnect_6700_firmware	Memory Corruption when invoking device input/output control operations for mapping and unmapping persistent memory buffers due to improper synchronization.	2026-07-06	6.6
CVE-2025-59616	qualcomm - fastconnect_6700_firmware	Memory Corruption when processing multiple IOCTL calls with the same buffer file descriptor input due to accessing already freed memory.	2026-07-06	6.6
CVE-2025-59617	qualcomm - fastconnect_6700_firmware	Memory Corruption when processing multiple IOCTL calls with the same buffer file descriptor input.	2026-07-06	6.6
CVE-2026-0287	paloaltonetworks - multiple products	Multiple denial of service vulnerabilities in Palo Alto Networks PAN-OS® software allow an unauthenticated attacker with network access to cause a denial of service (DoS) condition by sending specially crafted network traffic to or through a dataplane interface. Repeated attempts to trigger this condition result in the firewall entering maintenance mode. Panorama is not impacted by these vulnerabilities.	2026-07-09	6.6
CVE-2026-49086	apache - multiple products	Improper Input Validation, Unintended Proxy or Intermediary ('Confused Deputy') vulnerability in Apache Camel DAPR component. The camel-dapr Dapr Pub/Sub consumer (DaprPubSubConsumer) copied two fields from each inbound CloudEvent - its Pub/Sub component name and its topic - into the CamelDaprPubSubName and CamelDaprTopic Exchange headers. These two headers are producer-direction routing headers: when the route republishes through a Dapr producer, DaprConfigurationOptionsProxy reads them back and prefers them over the destination configured on the endpoint. As a result, in a route that consumes from one Dapr Pub/Sub topic and republishes to another (for example from('dapr-pubsub:p:t').to('dapr-pubsub:p:other')), an actor able to publish a message to the subscribed topic could set the CloudEvent's pub/sub-name and topic to values of their choosing and cause the re-published message to be delivered to an arbitrary Dapr Pub/Sub component and topic instead of the configured destination - redirecting or exfiltrating the message and bypassing the route's intended routing and any topic-level access controls in the underlying broker. Exploitation requires the ability to publish to the topic the route subscribes to; no other authentication or user interaction is needed. This issue affects Apache Camel: from 4.12.0 before 4.14.8, from 4.15.0 before 4.18.3, from 4.19.0 before 4.21.0. Users are recommended to upgrade to version 4.21.0, which fixes the issue. If users are on the 4.14.x LTS releases stream, then they are suggested to upgrade to 4.14.8. If users are on the 4.18.x releases stream, then they are suggested to upgrade to 4.18.3. For deployments that cannot upgrade immediately, remove the CamelDaprPubSubName and CamelDaprTopic headers from the Exchange between the Dapr consumer and any Dapr producer in the route (for example removeHeaders('CamelDaprPubSubName', 'CamelDaprTopic')), and restrict who can publish to the subscribed Dapr Pub/Sub topic so that only trusted producers can send to it.	2026-07-06	6.5
CVE-2026-49097	apache - multiple products	Improper Input Validation, Improper Neutralization of Special Elements in Output Used by a Downstream Component ('Injection') vulnerability in Apache Camel IRC component. The camel-irc producer chooses the destination of an outgoing IRC message from the irc.sendTo Exchange header (the constant IrcConstants.IRC_SEND_TO, value irc.sendTo); when that header is present it overrides the channel list configured on the endpoint, and the message is sent only to the specified destination. This and the component's other control headers (irc.target, irc.messageType, irc.user.*, irc.num, irc.value) used plain, non-Camel-prefixed values. Because these names do not start with the Camel / camel prefix, HttpHeaderFilterStrategy - which blocks only the Camel header namespace on the HTTP boundary - let them pass from an inbound HTTP request straight into the Exchange. In a route that bridges an HTTP consumer (for example platform-http) into an irc: producer, any HTTP client could therefore set the irc.sendTo header and redirect a message that the route intended for a configured channel to an arbitrary IRC channel or user - exfiltrating the message content to an attacker-chosen nickname, leaking it into a public channel, or delivering messages that appear to come from the bot. No credentials are required when the bridging consumer is unauthenticated. This issue affects Apache Camel: from 4.0.0 before 4.14.8, from 4.15.0 before 4.18.3, from 4.19.0 before 4.21.0. Users are recommended to upgrade to version 4.21.0, which fixes the issue. If users are on the 4.14.x LTS releases stream, then they are suggested to upgrade to 4.14.8. If users are on the 4.18.x releases stream, then they are suggested to upgrade to 4.18.3. After upgrading, routes that set IRC headers via the raw header names must use the CamelIrc* names (for example CamelIrcSendTo) instead of the old irc.* values. For deployments that cannot upgrade immediately, strip the irc.* headers from any untrusted ingress before the irc: producer (for example removeHeaders('irc.*') at the start of the route), and set the IRC destination from a trusted source.	2026-07-06	6.5
CVE-2026-48828	apache - airflow	The Bulk Variables API in Apache Airflow called the redactor without passing the variable's key, so the key-based `should_hide_value_for_key` check (which triggers on secret-suffixed key names like `*_password` / `*_token` / `*_secret`) could not fire for JSON-decodable variable values. An authenticated UI/API user with bulk Variable read permission could retrieve plaintext values from JSON variables whose key would otherwise trigger redaction. Affects deployments that store sensitive values in JSON-typed Airflow Variables under secret-	2026-07-07	6.5

		suffixed key names. Users are advised to upgrade to `apache-airflow` 3.3.0 or later (the fix landed on `main` after 3.2.2; no 3.2.x backport).		
CVE-2026-48892	apache - airflow	The Config API in Apache Airflow surfaced per-key secrets-backend overrides (environment variables like `AIRFLOW__SECRETS__BACKEND_KWARG__SECRET_ID` and `AIRFLOW__WORKERS__SECRETS_BACKEND_KWARG__SECRET_ID`) as synthetic config options whose option names were not in `sensitive_config_values`, so the masker did not redact them. An authenticated UI/API user with Config read permission could retrieve plaintext secrets-backend credentials (Vault `role_id` / `secret_id`, etc.) from the Config API output. Affects deployments that configure secrets backends via per-key environment overrides. Users are advised to upgrade to `apache-airflow` 3.3.0 or later.	2026-07-07	6.5
CVE-2026-49296	apache - airflow	Before apache-airflow 3.3.0, a user authorized to read one Dag could disclose the source of other Dags co-located in the same source file. `GET /api/v2/dagSources/{dag_id}` — and the equivalent Dag-source view in the UI — returned the entire source file without redacting Dags the caller was not authorized to read, bypassing per-DAG read authorization. Deployments that co-locate multiple Dags in a single file and rely on per-DAG access control to limit source visibility are affected; single-Dag-per-file deployments are not. Upgrade to apache-airflow 3.3.0 or later.	2026-07-07	6.5
CVE-2026-49487	apache - airflow	In Apache Airflow before 3.3.0, the REST API task-instance detail and list endpoints returned a deferred task's trigger kwargs without masking. When a deferred operator passed a secret (for example a provider API key) into its trigger, any authenticated user with DAG-scoped task-instance read access for that DAG could read that secret in clear text while the task was deferred. Users should upgrade to apache-airflow 3.3.0 or later, which masks sensitive values in trigger kwargs returned by the API.	2026-07-07	6.5
CVE-2025-12799	red hat - multiple products	A flaw was found in Jastow. Jastow is vulnerable to Cross-Site Scripting (XSS) attack. If using a set of combined configuration to allow unescaped characters in URL with embedded Undertow and Jastow, a server might be vulnerable to improper input handling.	2026-07-07	6.5
CVE-2026-44877	hewlett packard enterprise (hpe) - HPE Networking Instant On	An unauthenticated remote disclosure vulnerability has been identified in HPE Networking Instant On 1830, 1930, and 1960 Switches. Successful exploitation of this vulnerability could allow an unauthenticated remote threat actor to access sensitive cryptographic secrets on a vulnerable system.	2026-07-07	6.5
CVE-2026-60001	openbsd - openssh	sshd in OpenSSH before 10.4 does not always honor the minimum authentication delay.	2026-07-08	6.5
CVE-2026-15154	redhat - openshift_ai	A flaw was found in `guardrails-detectors`, a component of Red Hat OpenShift AI. This vulnerability, known as Regular Expression Denial of Service (ReDoS), allows a remote attacker to provide specially crafted regular expressions to the public detection API. This can cause catastrophic backtracking, leading to a worker process consuming 100% CPU indefinitely and resulting in a denial of service for the entire guardrails-mediated LLM pipeline.	2026-07-08	6.5
CVE-2026-15109	google - chrome	Uninitialized Use in ANGLE in Google Chrome prior to 150.0.7871.115 allowed a remote attacker to obtain potentially sensitive information from process memory via a crafted HTML page. (Chromium security severity: High)	2026-07-08	6.5
CVE-2026-40009	apache software foundation - Apache IoTDB	Improper Privilege Management, Improper Access Control vulnerability in Apache IoTDB. Authenticated users can escalate to full tree-path access by renaming themselves to __internal_auditor. This issue affects Apache IoTDB: from 2.0.8 before 2.0.10. Users are recommended to upgrade to version 2.0.10, which fixes the issue.	2026-07-10	6.5
CVE-2026-54468	dell - unisphere_for_powermax	Dell Unisphere for PowerMax, version(s) 10.3.0.5 and prior, contain(s) a path traversal vulnerability. A low privileged attacker with remote access could potentially exploit this vulnerability to read arbitrary files.	2026-07-10	6.5
CVE-2026-13239	drupal - WissKI	Missing Authorization vulnerability in Drupal WissKI allows Forceful Browsing. This issue affects WissKI versions: from 0.0.0 to 4.2.0.	2026-07-10	6.5
CVE-2026-13240	drupal - Paragraphs	Missing Authorization vulnerability in Drupal Paragraphs allows Forceful Browsing. This issue affects Paragraphs versions: from 0.0.0 to 1.21.0.	2026-07-10	6.5
CVE-2026-13241	drupal - Paragraphs	Missing Authorization vulnerability in Drupal Paragraphs allows Forceful Browsing. This issue affects Paragraphs versions: from 0.0.0 to 1.21.0.	2026-07-10	6.5
CVE-2026-13242	drupal - Geolocation Field	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in Drupal Geolocation Field allows SQL Injection. This issue affects Geolocation Field versions: from 0.0.0 to 3.15.0.	2026-07-10	6.5
CVE-2026-13356	mozilla - firefox	A malicious webpage could interrupt a pending navigation by enqueuing a synchronous JavaScript dialog, causing the browser UI to display the destination origin in the address bar while continuing to render attacker-controlled content. This vulnerability was fixed in Firefox for iOS 152.3.	2026-07-07	6.3
CVE-2026-15044	red hat - Red Hat OpenShift AI (RHOAI)	A flaw was found in the TrustyAI Service Operator. When deploying services like gorch or NemoGuardrails, if a specific security setting is not enabled, these services can expose their communication channels without requiring users to prove their identity. This allows any other program within the cluster to access the AI guardrails and orchestrator without proper authorization. An attacker could exploit this to gain unauthorized access to sensitive information and potentially make limited changes to the AI models.	2026-07-08	6.3
CVE-2026-15063	red hat - Red Hat OpenShift AI (RHOAI)	A flaw was found in the gorch service template, which is part of the trustyai-service-operator. Even when authentication is enabled, the gorch service exposes unproxied orchestrator and detector metrics ports. This allows any pod on the cluster network to directly access these ports, bypassing the kube-rbac-proxy and its authentication mechanisms. This could lead to unauthorized access to the orchestrator and detector metrics.	2026-07-08	6.3
CVE-2026-54800	siemens - multiple products	A vulnerability has been identified in CPCI85 Central Processing/Communication (All versions < V26.20), SICORE Base system (All versions < V26.20.0). The affected application ships with a default configuration that disables all OPC UA security mechanisms. This could allow an attacker to gain unauthorized access and control over critical system functions.	2026-07-09	6.3

CVE-2026-49844	apache - multiple products	Improper encoding of non-finite floating-point values during MapMessage JSON serialization in Apache Log4j API produces output that is not valid JSON. This issue affects Apache Log4j API versions 2.13.1 through 2.25.4 and version 2.26.0. The fix for CVE-2026-34481 did not cover all code paths: when a MapMessage contains a non-finite IEEE 754 value (NaN, Infinity, or -Infinity), MapMessage.asJson() emits the corresponding bare token. RFC 8259 does not permit these tokens, so a conformant parser rejects the resulting document. The defect is reachable only when both of the following conditions hold: * The application uses the message resolver https://logging.apache.org/log4j/2.x/manual/json-template-layout.html#event-template-resolver-message of JsonTemplateLayout or any other layout that relies on MapMessage.asJson() or MapMessage.getFormattedMessage(new String[]{"JSON"}). * The application logs a MapMessage that contains an attacker-controlled floating-point value. An attacker who can supply a non-finite value can cause the affected layout to emit malformed JSON, which may corrupt the enclosing log record or disrupt downstream log ingestion and parsing. Users are advised to upgrade to Apache Log4j API 2.25.5 or 2.26.1, both of which emit RFC 8259-compliant JSON for non-finite values.	2026-07-10	6.3
CVE-2025-8591	wso2 - multiple products	The software accepts user-supplied input via a URL parameter without adequate output encoding before reflecting it back to the user's browser. This condition allows an attacker to inject malicious script content into pages served by the application. By leveraging this weakness, an attacker can cause the user's browser to redirect to a malicious website, modify the UI of the webpage, or retrieve information from the browser. However, the impact is mitigated by the use of httpOnly flags on session-related cookies, preventing session hijacking.	2026-07-06	6.1
CVE-2026-15127	google - chrome	Inappropriate implementation in WebGL in Google Chrome prior to 150.0.7871.115 allowed a remote attacker to inject arbitrary scripts or HTML (UXSS) via a crafted HTML page. (Chromium security severity: High)	2026-07-08	6.1
CVE-2026-15128	google - chrome	Inappropriate implementation in Forms in Google Chrome prior to 150.0.7871.115 allowed a remote attacker to inject arbitrary scripts or HTML (UXSS) via a crafted HTML page. (Chromium security severity: High)	2026-07-08	6.1
CVE-2026-10770	drupal - Anti-Spam by CleanTalk	Improper Neutralization of Input During Web Page Generation ("Cross-site Scripting") vulnerability in Drupal Anti-Spam by CleanTalk allows Reflected XSS. This issue affects Anti-Spam by CleanTalk versions: from 0.0.0 to 9.7.1.	2026-07-10	6.1
CVE-2026-13231	drupal - Advanced Content Feedback (aka admin_feedback)	Improper Neutralization of Input During Web Page Generation ("Cross-site Scripting") vulnerability in Drupal Advanced Content Feedback (aka admin_feedback) allows Stored XSS. This issue affects Advanced Content Feedback (aka admin_feedback) versions: from 0.0.0 to 2.8.0.	2026-07-10	6.1
CVE-2026-13234	drupal - AI (Artificial Intelligence)	Improper Neutralization of Input During Web Page Generation ("Cross-site Scripting") vulnerability in Drupal AI (Artificial Intelligence) allows Cross-Site Scripting (XSS). This issue affects AI (Artificial Intelligence) versions: from 0.0.0 to 1.2.17, from 1.3.0 to 1.3.8, from 1.4.0 to 1.4.3.	2026-07-10	6.1
CVE-2026-58587	drupal - Drupal Canvas	Improper Neutralization of Input During Web Page Generation ("Cross-site Scripting") vulnerability in Drupal Drupal Canvas allows Cross-Site Scripting (XSS). This issue affects Drupal Canvas versions: from 0.0.0 to 1.4.2, from 1.5.0 to 1.5.2, from 1.6.0 to 1.6.1, from 1.7.0 to 1.7.1.	2026-07-10	6.1
CVE-2026-58588	drupal - Drupal Canvas	Improper Neutralization of Input During Web Page Generation ("Cross-site Scripting") vulnerability in Drupal Drupal Canvas allows Cross-Site Scripting (XSS). This issue affects Drupal Canvas versions: from 0.0.0 to 1.4.2, from 1.5.0 to 1.5.2, from 1.6.0 to 1.6.1, from 1.7.0 to 1.7.1.	2026-07-10	6.1
CVE-2026-58471	gnu - wget	GNU Wget through 1.25.0, fixed in commit c2640fe, contains a heap buffer overflow vulnerability in the convert_fname() function within src/url.c that allows remote attackers to trigger memory corruption through a server-supplied filename requiring character set conversion. When the output buffer is too small during iconv E2BIG reallocation, the reallocation logic miscalculates the remaining space, leading to a heap buffer overflow that can be exploited via a maliciously crafted server response.	2026-07-07	6
CVE-2026-58472	gnu - wget	GNU Wget through 1.25.0, fixed in commit dd692d9, contains a heap buffer overflow vulnerability in the html_quote_string() function in src/convert.c that allows a remote attacker to trigger memory corruption by supplying a crafted HTML attribute with a large number of characters requiring entity encoding. A server-supplied HTML attribute causes a signed integer counter to overflow during output size accumulation, resulting in an undersized heap allocation and subsequent heap buffer overflow during the copy phase.	2026-07-07	6
CVE-2026-0286	paloaltonetworks - multiple products	A command injection vulnerability in the management plane of Palo Alto Networks PAN-OS® software enables an authenticated administrator to execute arbitrary OS commands as root. The security risk posed by this issue is significantly minimized when CLI access is restricted to a limited group of administrators.	2026-07-09	6

		This issue is applicable to PAN-OS software on PA-Series and VM-Series firewalls and on Panorama (virtual and M-Series). Cloud NGFW and Prisma Access® are not impacted by this vulnerability.		
CVE-2026-57029	juniper - multiple products	A Missing Synchronization vulnerability in the flow collector handler of Juniper Networks Junos OS Evolved on QFX Series allows an adjacent, unauthenticated attacker to cause a Denial-of-Service (DoS). When the reachability of an sFlow collector changes, the corresponding next-hop entry is updated. If this update occurs simultaneously with the sFlow thread accessing the next-hop data (which is outside the attackers control), it causes the evo-pfemand process to crash, impacting all traffic forwarding until the automatic process restart has completed. This issue affects Junos OS Evolved on QFX Series: * all 23.2 versions, * 23.4 versions before 23.4R2-S7-EVO, * 24.2 versions before 24.2R2-S5-EVO, * 24.4 versions before 24.4R2-S3-EVO, * 25.2 versions before 25.2R2-EVO.	2026-07-09	6
CVE-2026-59999	openbsd - openssh	In sshd in OpenSSH before 10.4, DisableForwarding=yes was supposed to take precedence over PermitTunnel=yes, but did not.	2026-07-08	5.9
CVE-2026-55803	drupal - multiple products	Improperly Controlled Modification of Dynamically-Determined Object Attributes vulnerability in Drupal Drupal core allows Object Injection. This issue affects Drupal core versions: from 0.0.0 to 10.5.12, from 10.6.0 to 10.6.11, from 11.2.0 to 11.2.14, from 11.3.0 to 11.3.12, from 0.0.0 to 11.0.*, from 0.0.0 to 11.1.*.	2026-07-10	5.9
CVE-2026-55804	drupal - multiple products	Improperly Controlled Modification of Dynamically-Determined Object Attributes vulnerability in Drupal Drupal core allows Object Injection. This issue affects Drupal core versions: from 0.0.0 to 10.5.12, from 10.6.0 to 10.6.11, from 11.2.0 to 11.2.14, from 11.3.0 to 11.3.12, from 0.0.0 to 11.0.*, from 0.0.0 to 11.1.*.	2026-07-10	5.9
CVE-2026-55806	drupal - multiple products	URL Redirection to Untrusted Site ('Open Redirect') vulnerability in Drupal Drupal core allows Content Spoofing. This issue affects Drupal core versions: from 0.0.0 to 10.5.12, from 10.6.0 to 10.6.11, from 11.2.0 to 11.2.14, from 11.3.0 to 11.3.12, from 0.0.0 to 11.0.*, from 0.0.0 to 11.1.*.	2026-07-10	5.9
CVE-2026-11914	drupal - Composer	vulnerability in Drupal Composer allows . This issue affects Composer versions: *.*.	2026-07-10	5.9
CVE-2026-11915	drupal - Brute force attack protection	vulnerability in Drupal Brute force attack protection allows . This issue affects Brute force attack protection versions: *.*.	2026-07-10	5.9
CVE-2026-15086	drupal - Raw Formatter [Meta Tag Formatter]	vulnerability in Drupal Raw Formatter [Meta Tag Formatter] allows . This issue affects Raw Formatter [Meta Tag Formatter] versions: *.*.	2026-07-10	5.9
CVE-2026-15087	drupal - Clean RESTful	vulnerability in Drupal Clean RESTful allows . This issue affects Clean RESTful versions: *.*.	2026-07-10	5.9
CVE-2026-0278	paloaltonetworks - prisma_access_agent	Multiple protection mechanism failures in the Prisma Access Agent Data Loss Prevention (DLP) component for Windows allow a local user to bypass DLP policy enforcement controls. The Prisma Access Agent on macOS is not affected.	2026-07-09	5.8
CVE-2026-0277	paloaltonetworks - prisma_access_agent	An improper certificate validation vulnerability in the Prisma® Access Agent for iOS enables an attacker to perform a man-in-the-middle (MitM) attack to intercept VPN traffic. The Prisma Access Agent on Windows, macOS, Linux, Android and ChromeOS are not affected.	2026-07-09	5.7
CVE-2026-48267	adobe - dng_software_development_kit	DNG SDK versions 1.7.1 2536 and earlier are affected by a NULL Pointer Dereference vulnerability that could result in an application denial-of-service. An attacker could exploit this vulnerability to crash the application, leading to a denial-of-service condition. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	2026-07-06	5.5
CVE-2026-10769	drupal - Commerce Core	Improper Neutralization of Input During Web Page Generation ("Cross-site Scripting") vulnerability in Drupal Commerce Core allows Stored XSS. This issue affects Commerce Core versions: from 3.3.0 to 3.3.6.	2026-07-10	5.4
CVE-2026-11908	drupal - Tagify	Improper Neutralization of Input During Web Page Generation ("Cross-site Scripting") vulnerability in Drupal Tagify allows Stored XSS. This issue affects Tagify versions: from 0.0.0 to 1.2.52.	2026-07-10	5.4
CVE-2026-15079	drupal - Login Disable	Improper Restriction of Excessive Authentication Attempts vulnerability in Drupal Login Disable allows Brute Force. This issue affects Login Disable versions: from 0.0.0 to 2.1.4.	2026-07-10	5.4
CVE-2026-15082	drupal - Siteimprove Analytics	Improper Neutralization of Input During Web Page Generation ("Cross-site Scripting") vulnerability in Drupal Siteimprove Analytics allows Cross-Site Scripting (XSS). This issue affects Siteimprove Analytics versions: from 0.0.0 to 2.0.1.	2026-07-10	5.4
CVE-2026-15084	drupal - UI Patterns (SDC in Drupal UI)	Improper Neutralization of Input During Web Page Generation ("Cross-site Scripting") vulnerability in Drupal UI Patterns (SDC in Drupal UI) allows Stored XSS. This issue affects UI Patterns (SDC in Drupal UI) versions: from 2.0.0 to 2.0.17.	2026-07-10	5.4
CVE-2026-15085	drupal - AI SEO/GEO Analyzer	Improper Neutralization of Input During Web Page Generation ("Cross-site Scripting") vulnerability in Drupal AI SEO/GEO Analyzer allows Stored XSS. This issue affects AI SEO/GEO Analyzer versions: from 0.0.0 to 1.1.3.	2026-07-10	5.4

CVE-2026-55808	drupal - multiple products	Improper Neutralization of Input During Web Page Generation ("Cross-site Scripting") vulnerability in Drupal Drupal core allows Cross-Site Scripting (XSS). This issue affects Drupal core versions: from 0.0.0 to 10.5.12, from 10.6.0 to 10.6.11, from 11.2.0 to 11.2.14, from 11.3.0 to 11.3.12, from 0.0.0 to 11.0.*, from 0.0.0 to 11.1.*.	2026-07-10	5.4
CVE-2026-46453	apache - multiple products	Improper Input Validation, Authorization Bypass Through User-Controlled Key vulnerability in Apache Camel ElasticSearch Rest Client. The camel-elasticsearch-rest-client component reads several Exchange headers to control its behaviour - SEARCH_QUERY (an advanced query body), OPERATION (which Elasticsearch operation to run), INDEX_NAME, INDEX_SETTINGS and ID. The string values of these header constants, defined in ElasticSearchRestClientConstant, are plain unprefixed names ('SEARCH_QUERY', 'OPERATION', 'INDEX_NAME', 'INDEX_SETTINGS', 'ID') rather than the 'Camel'-prefixed names used by every other Camel component (for example CamelSqlQuery, CamelMongoDbCriteria, CamelCqlQuery). Camel's inbound HTTP header filter, HttpHeaderFilterStrategy, blocks only header names that begin with 'Camel' or 'camel'. Because the Elasticsearch header names do not carry that prefix, they pass through the inbound filter unchanged. When a Camel route exposes an HTTP entry point (for example platform-http) in front of an elasticsearch-rest-client producer, an untrusted HTTP client can set these headers directly on its request and override the query and operation that the route author configured: reading every document in the index (SEARCH_QUERY with a match_all query), deleting documents (OPERATION set to Delete together with ID), or exfiltrating selected fields. No credentials are required and the producer reads the headers unconditionally. This issue affects Apache Camel: from 4.3.0 before 4.14.8, from 4.15.0 before 4.18.3, from 4.19.0 before 4.21.0. Users are recommended to upgrade to version 4.21.0, which fixes the issue. If users are on the 4.14.x LTS releases stream, then they are suggested to upgrade to 4.14.8. If users are on the 4.18.x releases stream, then they are suggested to upgrade to 4.18.3. The fix renames the camel-elasticsearch-rest-client Exchange header constant string values (ID, SEARCH_QUERY, INDEX_SETTINGS, INDEX_NAME, OPERATION) to carry the Camel prefix (CamelElasticsearchId, CamelElasticsearchSearchQuery, CamelElasticsearchIndexSettings, CamelElasticsearchIndexName, CamelElasticsearchOperation) so that they are blocked by the inbound HttpHeaderFilterStrategy; the Java field names are unchanged. For deployments that cannot upgrade immediately, strip the affected headers from untrusted inbound messages before they reach the producer (for example removeHeader('SEARCH_QUERY'), removeHeader('OPERATION'), removeHeader('INDEX_NAME'), removeHeader('INDEX_SETTINGS') and removeHeader('ID') in front of the elasticsearch-rest-client endpoint), or apply a custom HeaderFilterStrategy that blocks these names.	2026-07-06	5.3
CVE-2026-48206	apache - multiple products	Improper Input Validation, Authorization Bypass Through User-Controlled Key vulnerability in Apache Camel JIRA component. The camel-jira producers read their operation parameters - the issue key, project key, transition id, summary, type, assignee, components, watchers, link type, work-log minutes and others - from Exchange message headers. The header constants defined in JiraConstants (for example ISSUE_KEY = IssueKey, ISSUE_PROJECT_KEY = ProjectKey, ISSUE_TRANSITION_ID = IssueTransitionId, LINK_TYPE = linkType) used plain, non-Camel-prefixed values. Because these names do not start with the Camel / camel prefix, HttpHeaderFilterStrategy - which blocks only the Camel header namespace on the HTTP boundary - let them pass from an inbound HTTP request straight into the Exchange. In a route that bridges an HTTP consumer (for example platform-http) into a jira: producer, any HTTP client could therefore supply these headers and override the values the route intended, driving JIRA operations against the configured JIRA instance with the endpoint's configured service-account credentials - for example deleting or transitioning an arbitrary issue (via IssueKey / IssueTransitionId), creating an issue in a different project (via ProjectKey), modifying issue fields, adding or removing watchers, or logging work. The operations are bounded by what the configured service account is permitted to do. No credentials are required from the attacker when the bridging consumer is unauthenticated. This issue affects Apache Camel: from 4.0.0 before 4.14.8, from 4.15.0 before 4.18.3, from 4.19.0 before 4.21.0. Users are recommended to upgrade to version 4.21.0, which fixes the issue. If users are on the 4.14.x LTS releases stream, then they are suggested to upgrade to 4.14.8. If users are on the 4.18.x releases stream, then they are suggested to upgrade to 4.18.3. After upgrading, routes that drive JIRA operations via the raw header names must use the CamelJira* names (for example CamelJiraIssueKey) instead of the old values. For deployments that cannot upgrade immediately, strip the camel-jira control headers from any untrusted ingress before the jira: producer (for example removing the IssueKey, ProjectKey, IssueTransitionId and related headers at the start of the route), and set the required JIRA operation parameters from a trusted source.	2026-07-06	5.3
CVE-2026-49098	apache - multiple products	Improper Input Validation, Improper Neutralization of Special Elements in Output Used by a Downstream Component ('Injection') vulnerability in Apache Camel Kafka Component. The camel-kafka producer can override its configured target topic at runtime from the kafka.OVERRIDE_TOPIC Exchange header: KafkaProducer.evaluateTopic() returns the header value in preference to the topic configured on the endpoint. The control-header constants in KafkaConstants (for example OVERRIDE_TOPIC = kafka.OVERRIDE_TOPIC, OVERRIDE_TIMESTAMP = kafka.OVERRIDE_TIMESTAMP, PARTITION_KEY = kafka.PARTITION_KEY) used plain, non-Camel-prefixed values. camel-kafka's own KafkaHeaderFilterStrategy does filter the kafka.* namespace, but only on the Kafka-to-Exchange serialization boundary (reading Kafka record headers into the Exchange, and writing Exchange headers into a Kafka record); it does not apply to headers that arrive from an	2026-07-06	5.3

		upstream consumer in a multi-component route. The upstream HTTP consumer uses HttpHeaderFilterStrategy, which blocks only the Camel / camel namespace, so a kafka.* header passes through unfiltered. As a result, in a route that bridges an HTTP consumer (for example platform-http) into a kafka: producer, any HTTP client could set the kafka.OVERRIDE_TOPIC header and cause the message to be published to an arbitrary Kafka topic instead of the configured one - redirecting it to a sensitive internal topic, or injecting attacker-crafted messages into a topic consumed by a critical downstream service. The related kafka.OVERRIDE_TIMESTAMP and kafka.PARTITION_KEY headers could likewise be injected to backdate messages or target specific partitions. No credentials are required when the bridging consumer is unauthenticated. This issue affects Apache Camel: from 4.0.0 before 4.14.8, from 4.15.0 before 4.18.3, from 4.19.0 before 4.21.0. Users are recommended to upgrade to version 4.21.0, which fixes the issue. If users are on the 4.14.x LTS releases stream, then they are suggested to upgrade to 4.14.8. If users are on the 4.18.x releases stream, then they are suggested to upgrade to 4.18.3. After upgrading, routes that set or read Kafka headers via the raw header names must use the CamelKafka* names (for example CamelKafkaOverrideTopic and CamelKafkaTopic) instead of the old kafka.* values. For deployments that cannot upgrade immediately, strip the kafka.* headers from any untrusted ingress before the kafka: producer (for example removeHeaders('kafka.*') at the start of the route), and set the target topic from a trusted source.		
CVE-2026-49099	apache - multiple products	Improper Neutralization of Special Elements in Output Used by a Downstream Component ('Injection'), Authorization Bypass Through User-Controlled Key vulnerability in Apache Camel Salesforce Component. The camel-salesforce producer resolves its operation parameters - the SOQL query, the SOSL search, the target SObject name and id, the Apex REST URL and method, and the Apex query parameters - from Exchange message headers, reading the header in preference to the value configured on the endpoint (AbstractSalesforceProcessor.getParameter() reads the header first and uses the endpoint configuration only as a fallback). The control-header constants in SalesforceEndpointConfig (for example SOBJECT_QUERY = sObjectQuery, SOBJECT_SEARCH = sObjectSearch, SOBJECT_NAME = sObjectName, SOBJECT_ID = sObjectId, APEX_URL = apexUrl, APEX_METHOD = apexMethod, and the apexQueryParam. prefix) used plain, non-Camel-prefixed values. Because these names do not start with the Camel / camel prefix, HttpHeaderFilterStrategy - which blocks only the Camel header namespace on the HTTP boundary - let them pass from an inbound HTTP request straight into the Exchange. In a route that bridges an HTTP consumer (for example platform-http) into a salesforce: producer, any HTTP client could therefore set these headers and override what the route intended - supplying its own SOQL query or SOSL search to read data from any SObject the connected Salesforce user can access, overriding the target SObject name and id for CRUD operations, or redirecting an Apex REST call to a different endpoint and HTTP method (including destructive methods) with injected query parameters. All such operations run with the full permissions of the Salesforce connected (integration) user, which is typically broad. No credentials are required from the attacker when the bridging consumer is unauthenticated. This issue affects Apache Camel: from 4.0.0 before 4.14.8, from 4.15.0 before 4.18.3, from 4.19.0 before 4.21.0. Users are recommended to upgrade to version 4.21.0, which fixes the issue. If users are on the 4.14.x LTS releases stream, then they are suggested to upgrade to 4.14.8. If users are on the 4.18.x releases stream, then they are suggested to upgrade to 4.18.3. After upgrading, routes that set Salesforce operation parameters via the raw header names must use the CamelSalesforce* names (for example CamelSalesforceSObjectQuery and CamelSalesforceApexUrl) instead of the old sObject* / apex* values; the endpoint-option spelling is unchanged. For deployments that cannot upgrade immediately, strip the Salesforce control headers from any untrusted ingress before the salesforce: producer (for example removeHeaders('sObject*') and removeHeaders('apex*') at the start of the route), and set the query, SObject and Apex parameters from a trusted source.	2026-07-06	5.3
CVE-2026-49365	apache - multiple products	Generation of Error Message Containing Sensitive Information vulnerability in Apache Camel Netty HTTP component. The camel-netty-http HTTP server consumer exposes a muteException option that controls what is returned to the client when a route processing error occurs. This option defaulted to false because the backing field was an uninitialised primitive boolean (Java's default of false), whereas the other Camel HTTP server components (camel-http / camel-jetty / camel-servlet and camel-platform-http) default it to true. With muteException=false, when a request triggers an exception during route processing the consumer writes the full Throwable stack trace into the HTTP response body as text/plain (via DefaultNettyHttpBinding) instead of returning an empty body. Any unauthenticated client that can reach the endpoint and cause a processing error - for example by sending a malformed request body, an invalid parameter, or otherwise triggering a route-internal failure - therefore receives a complete Java stack trace. Such a stack trace can disclose sensitive internal information, including credentials embedded in exception messages, internal host names and IP addresses, filesystem paths, dependency and version details, database and class names, and the application's internal structure, which an attacker can use to plan further attacks. This issue affects Apache Camel: from 4.0.0 before 4.14.8, from 4.15.0 before 4.18.3, from 4.19.0 before 4.21.0. Users are recommended to upgrade to version 4.21.0, which fixes the issue. If users are on the 4.14.x LTS releases stream, then they are suggested to upgrade to 4.14.8. If users are on the 4.18.x releases stream, then they are suggested to upgrade to 4.18.3. For deployments that cannot upgrade immediately, set muteException=true explicitly on the camel-netty-http	2026-07-06	5.3

		consumer (for example netty-http: http://0.0.0.0:8080/api?muteException=true , or globally via the camel.component.netty-http.configuration.mute-exception=true property), so that processing errors no longer return the stack trace to the client.		
CVE-2026-56139	apache - multiple products	Generation of Error Message Containing Sensitive Information vulnerability in Apache Camel Undertow Component. The camel-undertow HTTP server consumer exposes a muteException option that controls what is returned to the client when a route processing error occurs. This option defaulted to false, whereas the other Camel HTTP server components (camel-http / camel-jetty / camel-servlet and camel-platform-http) default it to true. With muteException=false, when a request triggers an exception during route processing the consumer writes the full Throwable stack trace into the HTTP response body as text/plain instead of returning an empty body. Any unauthenticated client that can reach the endpoint and cause a processing error - for example by sending a malformed request body, an invalid parameter, or otherwise triggering a route-internal failure - therefore receives a complete Java stack trace. Such a stack trace can disclose sensitive internal information, including credentials embedded in exception messages, internal host names and IP addresses, filesystem paths, dependency and version details, database and class names, and the application's internal structure, which an attacker can use to plan further attacks. In addition, for Rest DSL consumers the muteException option was not honoured at all: the RestUndertowHttpBinding was created with a hard-coded false, so the stack trace was returned even when muteException=true had been configured. This issue affects Apache Camel: from 4.0.0 before 4.14.8, from 4.15.0 before 4.18.3, from 4.19.0 before 4.21.0. Users are recommended to upgrade to version 4.21.0, which fixes the issue. If users are on the 4.14.x LTS releases stream, then they are suggested to upgrade to 4.14.8. If users are on the 4.18.x releases stream, then they are suggested to upgrade to 4.18.3. For deployments that cannot upgrade immediately, set muteException=true explicitly on the camel-undertow consumer (for example undertow: http://0.0.0.0:8080/api?muteException=true , or globally via the camel.component.undertow.mute-exception=true property), so that processing errors no longer return the stack trace to the client; note that on affected releases this workaround does not cover Rest DSL consumers, whose binding ignores the option until the fix is applied.	2026-07-06	5.3
CVE-2026-21368	qualcomm - fastconnect_6700_firmware	Memory Corruption when parsing jpeg commands due to unaccounted extra writes to the buffer during validation checks.	2026-07-06	5.3
CVE-2026-21369	qualcomm - fastconnect_6200_firmware	Memory Corruption when handling flash commands due to outdated LED count values being used after userspace modification.	2026-07-06	5.3
CVE-2026-21370	qualcomm - fastconnect_6700_firmware	Memory Corruption when validating input batch size and buffer plane count exceeds maximum allowed values.	2026-07-06	5.3
CVE-2026-21384	qualcomm - fastconnect_6700_firmware	Memory Corruption when updating prepared commands with invalid port indices based on user space input exceeds supported read client limits.	2026-07-06	5.3
CVE-2026-14940	redhat - multiple products	A heap-buffer-overflow flaw was found in 389 Directory Server (389-ds-base). When normalizing a Distinguished Name (DN) that contains a legacy-quoted value encoding a multivalued nested Relative Distinguished Name (RDN), the server can write past the end of a heap allocation while sorting RDN attribute-value pairs. An unauthenticated remote attacker can trigger this condition by sending an LDAP operation whose DN reaches the DN normalization routine, such as a search with a crafted base DN. This can corrupt heap memory and may cause denial of service.	2026-07-07	5.3
CVE-2026-33799	juniper - multiple products	An Out-of-bounds Write vulnerability in the SNMP daemon (snmpd) of Juniper Networks Junos OS and Junos OS Evolved allows an authenticated network-based attacker sending specific valid SNMPv3 queries to trigger a memory leak. Over time, continuous receipt of these queries will result in snmpd process memory exhaustion, resulting in a process crash and restart, impacting the ability to monitor the system via SNMP. Memory usage can be monitored using the following command: user@device> show system processes extensive | match snmpd This issue affects: Junos OS: * all versions before 21.2R3-S8; * from 21.4 before 21.4R3-S7; * from 22.1 before 22.1R3-S6; * from 22.2 before 22.2R3-S4; * from 22.3 before 22.3R3-S3; * from 22.4 before 22.4R3-S2; * from 23.2 before 23.2R2; * from 23.4 before 23.4R2. Junos OS Evolved:	2026-07-09	5.3

		* all versions before 21.2R3-S8-EVO; * from 21.4 before 21.4R3-S7-EVO; * all versions of 22.1-EVO, * from 22.2 before 22.2R3-S4-EVO; * from 22.3 before 22.3R3-S3-EVO; * all versions of 22.4-EVO, * from 23.2 before 23.2R2-EVO; * from 23.4 before 23.4R2-EVO.		
CVE-2026-54470	dell - unisphere_for_powermax	Dell Unisphere for PowerMax, version(s) 10.3.0.5 and prior contain(s) an Improper Restriction of XML External Entity Reference vulnerability. A low privileged attacker with remote access could potentially exploit this vulnerability, leading to Unauthorized access.	2026-07-10	5.3
CVE-2026-8609	grafana - multiple products	An unauthenticated attacker can repeatedly call Grafana's OAuth login route with unique values, causing unbounded memory growth that can eventually exhaust memory and crash the Grafana instance (denial of service).	2026-07-10	5.3
CVE-2026-14781	red hat - multiple products	A flaw exists in the org.keycloak.broker.oidc package where the OIDC broker incorrectly synchronizes the email_verified claim. When an OIDC identity provider is configured with trustEmail=true and the userinfo endpoint is enabled, Keycloak retrieves the email address from the userinfo response but retrieves the email_verified status exclusively from the id_token. The root cause is a lack of validation ensuring that the email_verified claim in the id_token actually refers to the email address returned by the userinfo endpoint. If these two sources return different email addresses, the id_token's email_verified=true claim is blindly applied to the userinfo email. Exploitation Conditions: The OIDC identity provider must have trustEmail set to true (non-default). The userinfo endpoint must be enabled (default). The attacker must control or have compromised the upstream OIDC provider. Concrete Impact: Mark arbitrary email addresses as verified in the Keycloak database. Bypass email-based security controls or verification workflows. Potential account takeover if the application relies solely on the email_verified flag from the IdP to link accounts.	2026-07-05	4.8
CVE-2026-59998	openbsd - openssh	sshd in OpenSSH before 10.4 has an undocumented security-relevant behavior: GSSAPIStrictAcceptorCheck has no value if the server is in Windows Active Directory.	2026-07-08	4.8
CVE-2026-13238	drupal - Commerce Realex / Global Payments	Incorrect Authorization vulnerability in Drupal Commerce Realex / Global Payments allows Forceful Browsing. This issue affects Commerce Realex / Global Payments versions: from 0.0.0 to 3.0.2.	2026-07-10	4.8
CVE-2026-13243	drupal - Salesforce Suite	Cross-Site Request Forgery (CSRF) vulnerability in Drupal Salesforce Suite allows Cross Site Request Forgery. This issue affects Salesforce Suite versions: from 0.0.0 to 5.1.3.	2026-07-10	4.8
CVE-2026-0284	paloaltonetworks - multiple products	An XML injection vulnerability in the Large Scale VPN (LSVPN) functionality of Palo Alto Networks PAN-OS® software enables an unauthenticated attacker with network access to inject malicious XML content, potentially leading to information disclosure or corruption of internal LSVPN satellite data. Panorama, Cloud NGFW, and Prisma® Access are not impacted by this vulnerability.	2026-07-09	4.7
CVE-2026-0285	paloaltonetworks - multiple products	A server-side request forgery (SSRF) vulnerability in Palo Alto Networks PAN-OS software enables an authenticated administrator with network access to the management web interface to make unauthorized requests from the firewall to internal services. The security risk posed by this issue is minimized when the management interface is restricted to only trusted internal IP addresses according to our recommended best practice deployment guidelines https://live.paloaltonetworks.com/t5/community-blogs/tips-amp-tricks-how-to-secure-the-management-access-of-your-palo/ba-p/464431 . Panorama, Cloud NGFW, and Prisma® Access are not impacted by this vulnerability.	2026-07-09	4.7
CVE-2026-56288	gnu - patch	GNU patch is vulnerable to a NULL pointer dereference when processing a specially crafted unified-diff patch file. Improper handling of consecutive end-of-file newline markers can corrupt internal hunk (single block of changes in diff) data structures, causing the application to pass a NULL pointer to fwrite() during patch processing. An attacker can trigger this condition with a malicious patch file, causing the utility to crash and resulting in a denial of service. This issue has been fixed in the commit e6d6a4e021660679d7fc9150f981d4920f722313	2026-07-09	4.6
CVE-2026-56289	gnu - patch	GNU patch is vulnerable to a denial of service (DoS) due to improper validation of hunk (single block of changes in diff) line offsets in unified-diff input. A specially crafted patch can specify an extremely large line number, causing the application to enter an effectively infinite processing loop while attempting to locate the requested position. This results in excessive CPU consumption and prevents the process from completing. An attacker can trigger this behavior by supplying a malicious patch file, causing the utility to become unresponsive and require manual termination.	2026-07-09	4.6

		This issue has been fixed in the commit faba04ef4f2b410257f76c1b9dc85e350929c4b9		
CVE-2026-0283	paloaltonetworks - multiple products	An authentication bypass vulnerability in Large Scale VPN (LSVPN) functionality of Palo Alto Networks PAN-OS software allows an attacker with network access to bypass security restrictions and establish an unauthorized site-to-site VPN connection. Panorama, Cloud NGFW, and Prisma® Access are not impacted by this vulnerability.	2026-07-09	4.5
CVE-2026-14969	redhat - multiple products	A flaw was found in 389-ds-base where the LDBM backend attribute encryption uses a hardcoded static initialization vector for AES-CBC and 3DES-CBC operations, allowing an attacker with privileged filesystem access to detect plaintext equality across encrypted entries by comparing ciphertext blocks.	2026-07-07	4.4
CVE-2026-48891	apache - airflow	A bug in Apache Airflow's `/ui/dependencies` scheduling graph endpoint applied the caller's readable-Dag filter to the top-level serialized Dag key but still emitted referenced Dag IDs through the `dep.source` and `dep.target` fields of trigger / sensor dependency entries. An authenticated UI user with read permission on some Dags could enumerate the identifiers of other Dags they were not authorized to read by inspecting the dependency graph for trigger / sensor references. Affects deployments that rely on per-Dag read scoping to keep Dag identifiers private across teams. This is a residual gap in the fix for CVE-2026-28563, which filtered the top-level Dag key but did not propagate the filter into the trigger / sensor dep-source / dep-target fields. Users who already upgraded for CVE-2026-28563 should additionally upgrade to `apache-airflow` 3.3.0 or later to cover the residual trigger / sensor dependency leak.	2026-07-07	4.3
CVE-2026-15108	google - chrome	Integer overflow in Extensions API in Google Chrome prior to 150.0.7871.115 allowed an attacker who convinced a user to install a malicious extension to perform an out of bounds memory read via a crafted Chrome Extension. (Chromium security severity: High)	2026-07-08	4.3
CVE-2026-15124	google - chrome	Insufficient policy enforcement in Passwords in Google Chrome prior to 150.0.7871.115 allowed a remote attacker to bypass same origin policy via a crafted HTML page. (Chromium security severity: High)	2026-07-08	4.3
CVE-2026-15130	google - chrome	Insufficient policy enforcement in Navigation in Google Chrome prior to 150.0.7871.115 allowed a remote attacker to bypass site isolation via a crafted HTML page. (Chromium security severity: High)	2026-07-08	4.3
CVE-2026-15131	google - chrome	Inappropriate implementation in Navigation in Google Chrome prior to 150.0.7871.115 allowed a remote attacker to bypass site isolation via a crafted HTML page. (Chromium security severity: Medium)	2026-07-08	4.3
CVE-2026-15080	drupal - Ray Enterprise Translation	Cross-Site Request Forgery (CSRF) vulnerability in Drupal Ray Enterprise Translation allows Cross Site Request Forgery. This issue affects Ray Enterprise Translation versions: from 0.0.0 to 4.0.4, from 4.1.0 to 4.1.4, from 11.0.0 to 11.0.4.	2026-07-10	4.3
CVE-2026-59995	openbsd - openssh	sftp in OpenSSH before 10.4 does not properly constrain the location of downloaded files when "sftp server:/path ." is used with an attacker-controlled server.	2026-07-08	4.2
CVE-2026-59996	openbsd - openssh	scp in OpenSSH before 10.4 may place a file in the parent directory of an intended directory when the copy occurs between two remote destinations.	2026-07-08	4.2
CVE-2026-59997	openbsd - openssh	internal-sftp in sshd in OpenSSH before 10.4 recognizes only the first 9 command-line arguments, which can be important if a later command-line argument would have helped to ensure the intended security properties of an SFTP connection.	2026-07-08	4.2
CVE-2026-15083	drupal - ECA: Event - Condition - Action	Improperly Controlled Modification of Dynamically-Determined Object Attributes vulnerability in Drupal ECA: Event - Condition - Action allows Object Injection. This issue affects ECA: Event - Condition - Action versions: from 0.0.0 to 2.1.20, from 3.0.0 to 3.0.12, from 3.1.0 to 3.1.4.	2026-07-10	4.2
CVE-2026-15028	red hat - multiple products	A flaw was found in libarchive. This vulnerability allows a remote attacker to trigger a heap overflow by providing a specially crafted tar archive. The issue occurs during the parsing of a PAX extended header containing a malformed SUN.holesdata sparse-file attribute. Successful exploitation could lead to a denial of service, making the system unavailable, or potentially allow for arbitrary code execution, giving the attacker control over the affected system.	2026-07-10	3.9
CVE-2026-59269	vmware - Pinniped	A user authenticating to Kubernetes clusters via the Pinniped Supervisor could potentially gain elevated permissions in the clusters, only if all the following conditions were true: the Pinniped Supervisor server is running with an ActiveDirectoryIdentityProvider resource configured; the ActiveDirectoryIdentityProvider.spec.groupSearch.attributes.groupName is empty; the attacker gains the ability to edit some part of the distinguished name (DN) of group entries in the Active Directory (AD) server's database for groups to which they belong; the configured group search parameters cause the edited group to be included in the group search results for the user; and the attacker knows the password for an AD user who belongs to the edited AD group. Affected versions: Pinniped (go.pinniped.dev) v0.11.0 through v0.46.0 inclusive; fixed in v0.47.0.	2026-07-09	3.8
CVE-2026-46584	apache - multiple products	Improper Input Validation, Exposure of Sensitive Information to an Unauthorized Actor vulnerability in Apache Camel Mail Component. The camel-mail producer (MailProducer.getSender) scanned the outgoing Exchange for message headers in the mail.smtp. / mail.smtps. namespace and, when any were present, built a per-message JavaMail sender with those values applied as JavaMail session properties, overriding the endpoint configuration. This namespace is Camel-internal - only MailProducer interprets it - and was not blocked by any HeaderFilterStrategy, so the values could originate from any inbound protocol (for example platform-http query parameters or request headers, or JMS / Kafka messages from untrusted producers) that feeds a route ending in an smtp / smtps producer without an intervening removeHeaders. The maximal impact is version-dependent: on releases before 4.19.0, setting mail.smtp.host redirects the SMTP connection to a server under the attacker's control, and because the producer then authenticates with the endpoint's configured username and password those credentials are transmitted to the attacker; on 4.19.0 and later the producer connects to the endpoint's configured host explicitly, so the reachable impact is limited to weakening transport security	2026-07-06	3.7

		(for example mail.smtp.ssl.trust, mail.smtp.starttls.enable or mail.smtp.socks.host) and interception of the outgoing message rather than host redirect. Exploitation requires a route that channels untrusted input into the mail producer without stripping the namespace. This issue affects Apache Camel: from 4.0.0 before 4.14.8, from 4.15.0 before 4.18.3, from 4.19.0 before 4.21.0. Users are recommended to upgrade to version 4.21.0, which fixes the issue. If users are on the 4.14.x LTS releases stream, then they are suggested to upgrade to 4.14.8. If users are on the 4.18.x releases stream, then they are suggested to upgrade to 4.18.3. After upgrading, the per-message override is disabled by default; enable it only on trusted endpoints with useJavaMailSessionPropertiesFromHeaders=true. For deployments that cannot upgrade immediately, strip the namespace before the mail producer with removeHeaders('mail.smtp.*') and removeHeaders('mail.smtps.*') between any untrusted ingress and the smtp / smtps producer. Even with the opt-in enabled, route authors should still strip the namespace on any path that carries untrusted input.		
CVE-2026-14935	red hat - multiple products	A logic vulnerability was found in GStreamer's webrtcbin component. The _check_sdp_crypto() function contains an inverted boolean condition that causes it to accept remote SDP offers or answers that lack the required a=fingerprint attribute, while incorrectly rejecting those that include it. An attacker with the ability to intercept and modify WebRTC signaling messages could exploit this to bypass the SDP-level DTLS certificate fingerprint binding, weakening defenses against man-in-the-middle attacks on media streams.	2026-07-07	3.7
CVE-2026-60000	openbsd - openssh	sshd in OpenSSH before 10.4 allows remote attackers to cause a denial of service (resource consumption from excessive authentication attempts) because MaxAuthTries was mishandled for GSSAPIAuthentication.	2026-07-08	3.7
CVE-2026-15041	redhat - multiple products	A flaw was found in 389 Directory Server. The PBKDF2-SHA256 password verification function uses standard memcmp() for comparing password hashes instead of a constant-time comparison function. A remote attacker could potentially use timing measurements of LDAP bind attempts to infer partial hash information, though practical exploitation is extremely difficult due to PBKDF2 computational overhead.	2026-07-08	3.7
CVE-2026-15115	google - chrome	Insufficient validation of untrusted input in WebAppInstalls in Google Chrome on Android prior to 150.0.7871.115 allowed a local attacker to bypass same origin policy via a crafted HTML page. (Chromium security severity: High)	2026-07-08	3.3
CVE-2026-11909	drupal - Examples for Developers	Missing Authorization vulnerability in Drupal Examples for Developers allows Forceful Browsing. This issue affects Examples for Developers versions: from 0.0.0 to 4.0.6.	2026-07-10	3.3
CVE-2026-13233	drupal - OpenAI Provider	Server-Side Request Forgery (SSRF) vulnerability in Drupal OpenAI Provider allows Server Side Request Forgery. This issue affects OpenAI Provider versions: from 0.0.0 to 1.1.1, from 1.2.0 to 1.2.2.	2026-07-10	3.3
CVE-2026-28378	grafana - multiple products	The public dashboard deletion endpoint does not enforce organization isolation, allowing an Org Admin in one organization to delete public dashboards belonging to a different organization by supplying the target dashboard's identifiers.	2026-07-07	3.1
CVE-2026-13232	drupal - Advanced Content Feedback (aka admin_feedback)	Incorrect Authorization vulnerability in Drupal Advanced Content Feedback (aka admin_feedback) allows Forceful Browsing. This issue affects Advanced Content Feedback (aka admin_feedback) versions: from 0.0.0 to 2.8.0.	2026-07-10	3.1
CVE-2026-55807	drupal - multiple products	Server-Side Request Forgery (SSRF) vulnerability in Drupal Drupal core allows Server Side Request Forgery. This issue affects Drupal core versions: from 0.0.0 to 10.5.12, from 10.6.0 to 10.6.11, from 11.2.0 to 11.2.14, from 11.3.0 to 11.3.12, from 0.0.0 to 11.0.*, from 0.0.0 to 11.1.*.	2026-07-10	3.1
CVE-2026-53480	dell - multiple products	Dell PowerProtect Data Domain, versions 7.7.1.0 through 8.7, LTS2026 release version 8.6.1.0 through 8.6.1.10, LTS2025 release version 8.3.1.0 through 8.3.1.30, LTS2024 release versions 7.13.1.0 through 7.13.1.70 contain an improper limitation of a pathname to a restricted directory ('path traversal') vulnerability. A high privileged attacker with remote access could potentially exploit this vulnerability, leading to unauthorized file modification.	2026-07-08	2.7
CVE-2026-0282	paloaltonetworks - multiple products	A file deletion vulnerability in Palo Alto Networks PAN-OS® software enables an unauthenticated attacker with network access to the management web interface to delete files from a temporary directory. The security risk posed by this issue is minimized by restricting access to the management web interface to only trusted internal IP addresses according to our recommended best practice deployment guidelines https://live.paloaltonetworks.com/t5/community-blogs/tips-amp-tricks-how-to-secure-the-management-access-of-your-palo/ba-p/464431 . This issue is applicable to PAN-OS software on PA-Series and VM-Series firewalls and on Panorama (virtual and M-Series). Cloud NGFW and Prisma® Access are not impacted by this vulnerability.	2026-07-09	2.7
CVE-2026-0281	paloaltonetworks - multiple products	An information disclosure vulnerability in Palo Alto Networks PAN-OS® software enables an unauthenticated attacker with network access to the management web interface to obtain web session tokens. This requires a legitimate user to first click on a malicious link provided by the attacker. The security risk posed by this issue is minimized by restricting access to the management web interface to only trusted internal IP addresses according to our recommended best practice deployment guidelines https://live.paloaltonetworks.com/t5/community-blogs/tips-amp-tricks-how-to-secure-the-management-access-of-your-palo/ba-p/464431 . This issue is applicable to PAN-OS software on PA-Series and VM-Series firewalls and on Panorama (virtual and M-Series). Cloud NGFW and Prisma® Access are not impacted by this vulnerability.	2026-07-09	2.1

CVE-2026-0275	paloaltonetworks - prisma_browser	A local privilege escalation vulnerability in Palo Alto Networks Prisma® Browser allows a locally authenticated administrator with access to the macOS local filesystem to perform actions on the device with root privileges. This issue only affects Prisma® Browser on macOS.	2026-07-09	2
CVE-2026-15182	gnu - LibreDWG	A vulnerability has been found in GNU LibreDWG up to 0.13.4. The affected element is the function dwg_bmp of the file src/dwg.c of the component BMP Image Handler. Such manipulation leads to heap-based buffer overflow. The attack must be carried out locally. The exploit has been disclosed to the public and may be used. Upgrading to version 0.14 is sufficient to fix this issue. The name of the patch is 18fd542bb4d5ccedf9de12052bf50068b2b26f06. It is suggested to upgrade the affected component.	2026-07-09	1.9
CVE-2026-15184	gnu - LibreDWG	A vulnerability was found in GNU LibreDWG up to 0.13.4. The impacted element is the function dwg_next_entity of the file src/dwg.c of the component DWG File Handler. Performing a manipulation of the argument next_obj results in null pointer dereference. The attack must be initiated from a local position. The exploit has been made public and could be used. Upgrading to version 0.14 is sufficient to resolve this issue. The patch is named dde45dac3c4d902e4d8fed150a8017b9732019c9. Upgrading the affected component is recommended. Different than CVE-2026-9503.	2026-07-09	1.9
CVE-2026-0280	paloaltonetworks - multiple products	An IPv6 packet processing vulnerability in the dataplane of Palo Alto Networks PAN-OS® software enables an unauthenticated attacker to bypass firewall security policy enforcement, allowing network traffic that should be blocked to reach protected services. Cloud NGFW and Panorama are not impacted by this vulnerability.	2026-07-09	1.7
CVE-2026-0279	paloaltonetworks - multiple products	Multiple cross site scripting vulnerabilities in the User-ID™ Authentication Portal (aka Captive Portal) service, GlobalProtect™ gateway/portal features and Clientless VPN of Palo Alto Networks PAN-OS® software enables a malicious unauthenticated user to store or execute malicious JavaScript payload. The security risk posed by this issue is minimized when the management interface and access to the User-ID™ Authentication Portal is restricted to only trusted internal IP addresses according to our recommended best practice deployment guidelines https://live.paloaltonetworks.com/t5/community-blogs/tips-amp-tricks-how-to-secure-the-management-access-of-your-palo/ba-p/464431 . This issue is applicable to PAN-OS software on PA-Series and VM-Series firewalls and on Panorama (virtual and M-Series). Cloud NGFW is not affected by this vulnerability.	2026-07-09	1.3
CVE-2026-0276	paloaltonetworks - cortex_xdr_broker_vm	A privilege escalation vulnerability in Palo Alto Networks Cortex® XDR Broker VM enables a locally authenticated user to perform actions as the root user.	2026-07-09	1.1

Where NCA provides the vulnerability information as published by NIST's NVD. In addition, it is the entity's or individual's responsibility to ensure the implementation of appropriate recommendations.

وحيث تقدم الهيئة تفاصيل الثغرات كما تم نشرها من قبل NIST's NVD. وإذ تبقى مسؤولية الجهة أو الشخص قائمة للتأكد من تطبيق التوصيات المناسبة.