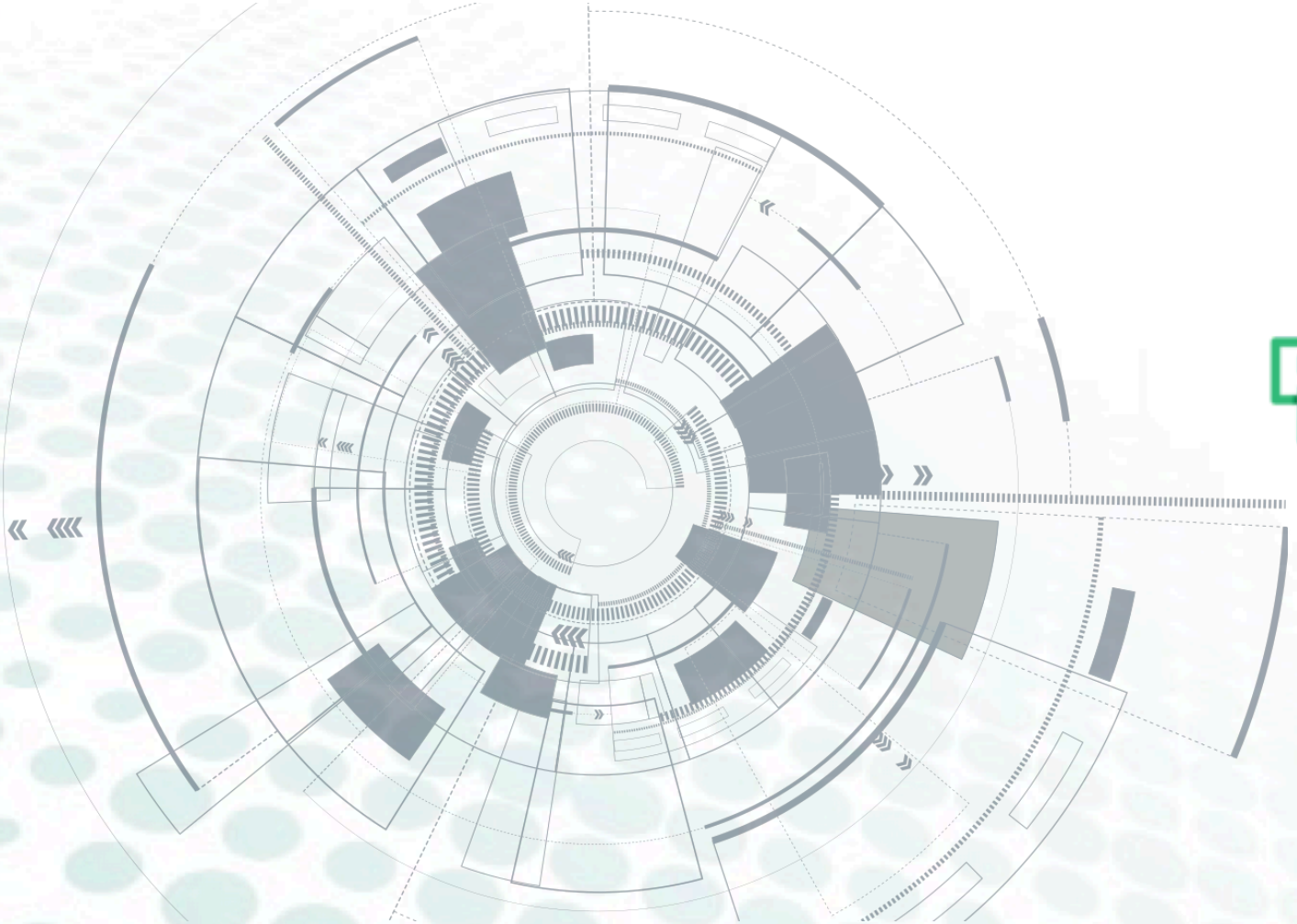

NeuVector
BY SUSE

Vulnerability reports (Vulnerability View)

Summary

Details

Name	Description	Score	Packages	Published at	Impact
CVE-2026-22796	Issue summary: A type confusion vulnerability exists in the signature verification of signed PKCS#7 data where an ASN1_TYPE union member is accessed without first validating the type, causing an invalid or NULL pointer dereference when processing malformed PKCS#7 data. Impact summary: An application performing signature verification of PKCS#7 data or calling directly the PKCS7_digest_from_attributes() function can be caused to dereference an invalid or NULL pointer when reading, resulting in a Denial of Service. The function PKCS7_digest_from_attributes() accesses the message digest attribute value without validating its type. When the type is not V_ASN1_OCTET_STRING, this results in accessing invalid memory through the ASN1_TYPE union, causing a crash. Exploiting this vulnerability requires an attacker to provide a malformed signed PKCS#7 to an application that verifies it. The impact of the exploit is just a Denial of Service, the PKCS7 API is legacy and applications should be using the CMS API instead. For these reasons the issue was assessed as Low severity. The FIPS modules in 3.5, 3.4, 3.3 and 3.0 are not affected by this issue, as the PKCS#7 parsing implementation is outside the OpenSSL FIPS module boundary.	V2: 4 V3: 5.3	openssl Impacted Version: 3.5.1-r0 — Fixed Version: 3.5.5-r0 Impacted Version: 3.5.4-r0 — Fixed Version: 3.5.5-r0	Jan 27, 2026 09:46:35	**Containers** argocd-redis-7fd4c97dd4-d4fr8 argocd-dex-server-88bbf995c-92jj7 **Images** ecr-public.aws.com/docker/library/redis:8.2.2-alpine ghcr.io/dexidp/dex:v2.44.0

Name	Description	Score	Packages	Published at	Impact
	OpenSSL 3.6, 3.5, 3.4, 3.3, 3.0, 1.1.1 and 1.0.2 are vulnerable to this issue.				
CVE-2025-9232	Issue summary: An application using the OpenSSL HTTP client API functions may trigger an out-of-bounds read if the 'no_proxy' environment variable is set and the host portion of the authority component of the HTTP URL is an IPv6 address. Impact summary: An out-of-bounds read can trigger a crash which leads to Denial of Service for an application. The OpenSSL HTTP client API functions can be used directly by applications but they are also used by the OCSP client functions and CMP (Certificate Management Protocol) client implementation in OpenSSL. However the URLs used by these implementations are unlikely to be controlled by an attacker. In this vulnerable code the out of bounds read can only trigger a crash. Furthermore the vulnerability requires an attacker-controlled URL to be passed from an application to the OpenSSL function and the user has to have a 'no_proxy' environment variable set. For the aforementioned reasons the issue was assessed as Low severity. The vulnerable code was introduced in the following patch releases: 3.0.16, 3.1.8, 3.2.4, 3.3.3, 3.4.0 and 3.5.0. The FIPS modules in 3.5, 3.4, 3.3, 3.2, 3.1 and 3.0 are not affected by this issue, as the HTTP client implementation is outside the OpenSSL FIPS module boundary.	V2: 4 V3: 5.9	openssl Impacted Version: 3.5.1-r0 Fixed Version: 3.5.4-r0	Sep 30, 2025 07:45:41	**Containers** argocd-dex-server-88bbf995c-92jj7 **Images** ghcr.io/dexidp/dex:v2.44.0

Name	Description	Score	Packages	Published at	Impact
CVE-2025-9231	Issue summary: A timing side-channel which could potentially allow remote recovery of the private key exists in the SM2 algorithm implementation on 64 bit ARM platforms. Impact summary: A timing side-channel in SM2 signature computations on 64 bit ARM platforms could allow recovering the private key by an attacker.. While remote key recovery over a network was not attempted by the reporter, timing measurements revealed a timing signal which may allow such an attack. OpenSSL does not directly support certificates with SM2 keys in TLS, and so this CVE is not relevant in most TLS contexts. However, given that it is possible to add support for such certificates via a custom provider, coupled with the fact that in such a custom provider context the private key may be recoverable via remote timing measurements, we consider this to be a Moderate severity issue. The FIPS modules in 3.5, 3.4, 3.3, 3.2, 3.1 and 3.0 are not affected by this issue, as SM2 is not an approved algorithm.	V2: 4 V3: 6.5	openssl Impacted Version: 3.5.1-r0 Fixed Version: 3.5.4-r0	Sep 30, 2025 07:45:41	**Containers** argocd-dex-server-88bbf995c-92jj7 **Images** ghcr.io/dexidp/dex:v2.44.0

Name	Description	Score	Packages	Published at	Impact
CVE-2025-9230	Issue summary: An application trying to decrypt CMS messages encrypted using password based encryption can trigger an out-of-bounds read and write. Impact summary: This out-of-bounds read may trigger a crash which leads to Denial of Service for an application. The out-of-bounds write can cause a memory corruption which can have various consequences including a Denial of Service or Execution of attacker-supplied code. Although the consequences of a successful exploit of this vulnerability could be severe, the probability that the attacker would be able to perform it is low. Besides, password based (PWRI) encryption support in CMS messages is very rarely used. For that reason the issue was assessed as Moderate severity according to our Security Policy. The FIPS modules in 3.5, 3.4, 3.3, 3.2, 3.1 and 3.0 are not affected by this issue, as the CMS implementation is outside the OpenSSL FIPS module boundary.	V2: 7 V3: 7.5	openssl Impacted Version: 3.5.1-r0 Fixed Version: 3.5.4-r0	Sep 30, 2025 07:45:41	**Containers** argocd-dex-server-88bbf995c-92jj7 **Images** ghcr.io/dexidp/dex:v2.44.0

Name	Description	Score	Packages	Published at	Impact
CVE-2025-69420	Issue summary: A type confusion vulnerability exists in the TimeStamp Response verification code where an ASN1_TYPE union member is accessed without first validating the type, causing an invalid or NULL pointer dereference when processing a malformed TimeStamp Response file. Impact summary: An application calling TS_RESP_verify_response() with a malformed TimeStamp Response can be caused to dereference an invalid or NULL pointer when reading, resulting in a Denial of Service. The functions ossl_ess_get_signing_cert() and ossl_ess_get_signing_cert_v2() access the signing cert attribute value without validating its type. When the type is not V_ASN1_SEQUENCE, this results in accessing invalid memory through the ASN1_TYPE union, causing a crash. Exploiting this vulnerability requires an attacker to provide a malformed TimeStamp Response to an application that verifies timestamp responses. The TimeStamp protocol (RFC 3161) is not widely used and the impact of the exploit is just a Denial of Service. For these reasons the issue was assessed as Low severity. The FIPS modules in 3.5, 3.4, 3.3 and 3.0 are not affected by this issue, as the TimeStamp Response implementation is outside the OpenSSL FIPS module boundary. OpenSSL 3.6, 3.5, 3.4, 3.3, 3.0 and 1.1.1 are vulnerable to this issue.	V2: 7 V3: 7.5	openssl Impacted Version: 3.5.1-r0 — Fixed Version: 3.5.5-r0 Impacted Version: 3.5.4-r0 — Fixed Version: 3.5.5-r0	Jan 27, 2026 09:46:34	**Containers** argocd-redis-7fd4c97dd4-d4fr8 argocd-dex-server-88bbf995c-92jj7 **Images** ecr-public.aws.com/docker/library/redis:8.2.2-alpine ghcr.io/dexidp/dex:v2.44.0

Name	Description	Score	Packages	Published at	Impact
	OpenSSL 1.0.2 is not affected by this issue.				

Name	Description	Score	Packages	Published at	Impact
CVE-2025-69419	Issue summary: Calling PKCS12_get_friendlyname() function on a maliciously crafted PKCS#12 file with a BMPString (UTF-16BE) friendly name containing non-ASCII BMP code point can trigger a one byte write before the allocated buffer. Impact summary: The out-of-bounds write can cause a memory corruption which can have various consequences including a Denial of Service. The OPENSSL_uni2utf8() function performs a two-pass conversion of a PKCS#12 BMPString (UTF-16BE) to UTF-8. In the second pass, when emitting UTF-8 bytes, the helper function bmp_to_utf8() incorrectly forwards the remaining UTF-16 source byte count as the destination buffer capacity to UTF8_putc(). For BMP code points above U+07FF, UTF-8 requires three bytes, but the forwarded capacity can be just two bytes. UTF8_putc() then returns -1, and this negative value is added to the output length without validation, causing the length to become negative. The subsequent trailing NUL byte is then written at a negative offset, causing write outside of heap allocated buffer. The vulnerability is reachable via the public PKCS12_get_friendlyname() API when parsing attacker-controlled PKCS#12 files. While PKCS12_parse() uses a different code path that avoids this issue, PKCS12_get_friendlyname() directly	V2: 7 V3: 7.4	openssl Impacted Version / Fixed Version 3.5.1-r0 / 3.5.5-r0 3.5.4-r0 / 3.5.5-r0	Jan 27, 2026 09:46:34	**Containers** argocd-redis-7fd4c97dd4-d4fr8 argocd-dex-server-88bbf995c-92jj7 **Images** ecr-public.aws.com/docker/library/redis:8.2.2-alpine ghcr.io/dexidp/dex:v2.44.0

Name	Description	Score	Packages	Published at	Impact
	invokes the vulnerable function. Exploitation requires an attacker to provide a malicious PKCS#12 file to be parsed by the application and the attacker can just trigger a one zero byte write before the allocated buffer. For that reason the issue was assessed as Low severity according to our Security Policy. The FIPS modules in 3.6, 3.5, 3.4, 3.3 and 3.0 are not affected by this issue, as the PKCS#12 implementation is outside the OpenSSL FIPS module boundary. OpenSSL 3.6, 3.5, 3.4, 3.3, 3.0 and 1.1.1 are vulnerable to this issue. OpenSSL 1.0.2 is not affected by this issue.				

Name	Description	Score	Packages	Published at	Impact
CVE-2025-69418	Issue summary: When using the low-level OCB API directly with AES-NI or other hardware-accelerated code paths, inputs whose length is not a multiple of 16 bytes can leave the final partial block unencrypted and unauthenticated. Impact summary: The trailing 1-15 bytes of a message may be exposed in cleartext on encryption and are not covered by the authentication tag, allowing an attacker to read or tamper with those bytes without detection. The low-level OCB encrypt and decrypt routines in the hardware-accelerated stream path process full 16-byte blocks but do not advance the input/output pointers. The subsequent tail-handling code then operates on the original base pointers, effectively reprocessing the beginning of the buffer while leaving the actual trailing bytes unprocessed. The authentication checksum also excludes the true tail bytes. However, typical OpenSSL consumers using EVP are not affected because the higher-level EVP and provider OCB implementations split inputs so that full blocks and trailing partial blocks are processed in separate calls, avoiding the problematic code path. Additionally, TLS does not use OCB ciphersuites. The vulnerability only affects applications that call the low-level CRYPTO_ocb128_encrypt() or CRYPTO_ocb128_decrypt() functions directly with non-block-aligned lengths in a single call on hardware-accelerated builds. For these reasons the issue was assessed as Low severity. The FIPS modules in 3.6, 3.5, 3.4, 3.3, 3.2, 3.1 and 3.0 are not affected by this issue, as OCB mode is not a FIPS-approved algorithm. OpenSSL 3.6, 3.5, 3.4, 3.3, 3.0 and 1.1.1 are vulnerable to this issue. OpenSSL 1.0.2 is not affected by this issue.	V2: 4 V3: 4	openssl Impacted Version / Fixed Version 3.5.1-r0 / 3.5.5-r0 3.5.4-r0 / 3.5.5-r0	Jan 27, 2026 09:46:33	**Containers** argocd-redis-7fd4c97dd4-d4fr8 argocd-dex-server-88bbf995c-92jj7 **Images** ecr-public.aws.com/docker/library/redis:8.2.2-alpine ghcr.io/dexidp/dex:v2.44.0

Name	Description	Score	Packages	Published at	Impact
CVE-2025-68160	Issue summary: Writing large, newline-free data into a BIO chain using the line-buffering filter where the next BIO performs short writes can trigger a heap-based out-of-bounds write. Impact summary: This out-of-bounds write can cause memory corruption which typically results in a crash, leading to Denial of Service for an application. The line-buffering BIO filter (BIO_f_linebuffer) is not used by default in TLS/SSL data paths. In OpenSSL command-line applications, it is typically only pushed onto stdout/stderr on VMS systems. Third-party applications that explicitly use this filter with a BIO chain that can short-write and that write large, newline-free data influenced by an attacker would be affected. However, the circumstances where this could happen are unlikely to be under attacker control, and BIO_f_linebuffer is unlikely to be handling non-curated data controlled by an attacker. For that reason the issue was assessed as Low severity. The FIPS modules in 3.6, 3.5, 3.4, 3.3 and 3.0 are not affected by this issue, as the BIO implementation is outside the OpenSSL FIPS module boundary. OpenSSL 3.6, 3.5, 3.4, 3.3, 3.0, 1.1.1 and 1.0.2 are vulnerable to this issue.	V2: 4 V3: 4.7	openssl Impacted Version: 3.5.1-r0 — Fixed Version: 3.5.5-r0 Impacted Version: 3.5.4-r0 — Fixed Version: 3.5.5-r0	Jan 27, 2026 09:46:15	**Containers** argocd-redis-7fd4c97dd4-d4fr8 argocd-dex-server-88bbf995c-92jj7 **Images** ecr-public.aws.com/docker/library/redis:8.2.2-alpine ghcr.io/dexidp/dex:v2.44.0

Name	Description	Score	Packages	Published at	Impact
CVE-2025-66199	Issue summary: A TLS 1.3 connection using certificate compression can be forced to allocate a large buffer before decompression without checking against the configured certificate size limit. Impact summary: An attacker can cause per-connection memory allocations of up to approximately 22 MiB and extra CPU work, potentially leading to service degradation or resource exhaustion (Denial of Service). In affected configurations, the peer-supplied uncompressed certificate length from a CompressedCertificate message is used to grow a heap buffer prior to decompression. This length is not bounded by the max_cert_list setting, which otherwise constrains certificate message sizes. An attacker can exploit this to cause large per-connection allocations followed by handshake failure. No memory corruption or information disclosure occurs. This issue only affects builds where TLS 1.3 certificate compression is compiled in (i.e., not OPENSSL_NO_COMP_ALG) and at least one compression algorithm (brotli, zlib, or zstd) is available, and where the compression extension is negotiated. Both clients receiving a server CompressedCertificate and servers in mutual TLS scenarios receiving a client CompressedCertificate are affected. Servers that do not request client certificates are not vulnerable to client-initiated attacks.	V2: 4 V3: 5.9	openssl Impacted Version: 3.5.1-r0 — Fixed Version: 3.5.5-r0 Impacted Version: 3.5.4-r0 — Fixed Version: 3.5.5-r0	Jan 27, 2026 09:46:15	**Containers** argocd-redis-7fd4c97dd4-d4fr8 argocd-dex-server-88bbf995c-92jj7 **Images** ecr-public.aws.com/docker/library/redis:8.2.2-alpine ghcr.io/dexidp/dex:v2.44.0

Name	Description	Score	Packages	Published at	Impact
	Users can mitigate this issue by setting SSL_OP_NO_RX_CERTIFICATE_COMPRESSION to disable receiving compressed certificates. The FIPS modules in 3.6, 3.5, 3.4 and 3.3 are not affected by this issue, as the TLS implementation is outside the OpenSSL FIPS module boundary. OpenSSL 3.6, 3.5, 3.4 and 3.3 are vulnerable to this issue. OpenSSL 3.0, 1.1.1 and 1.0.2 are not affected by this issue.				

Name	Description	Score	Packages	Published at	Impact
CVE-2025-64329	containerd CRI server: Host memory exhaustion through Attach goroutine leak ### Impact A bug was found in containerd's CRI Attach implementation where a user can exhaust memory on the host due to goroutine leaks. Repetitive calls of CRI Attach (e.g., [`kubectl attach`](https://kubernetes.io/docs/reference/kubectl/generated/kubectl_attach/)) could increase the memory usage of containerd. ### Patches This bug has been fixed in the following containerd versions: * 2.2.0 * 2.1.5 * 2.0.7 * 1.7.29 Users should update to these versions to resolve the issue. ### Workarounds Set up an admission controller to control accesses to `pods/attach` resources. e.g., [Validating Admission Policy](https://kubernetes.io/docs/reference/access-authn-authz/validating-admission-policy/). ### Credits The containerd project would like to thank @Wheat2018 for responsibly disclosing this issue in accordance with the [containerd security policy](https://github.com/containerd/project/blob/main/SECURITY.md). ### References https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2025-64329 ### For more information	V2: 4 V3: 5.5	go:github.com/containerd/containerd Impacted Version: 1.7.27 Fixed Version: 1.7.29	Nov 7, 2025 05:02:23	**Containers** argocd-application-controller-0 argocd-notifications-controller-7cf65d89f6-cqwj2 argocd-server-6c66b766f5-6f9vv argocd-applicationset-controller-6d68c66d6d-wdxlg argocd-repo-server-77977bc6f9-22bck **Images** quay.io/argoproj/argocd:v3.2.5

<table>
<tr><th>Name</th><th>Description</th><th>Score</th><th>Packages</th><th>Published at</th><th>Impact</th></tr>
<tr><td></td><td>If you have any questions or comments about this advisory:
* Open an issue in [containerd] (https://github.com/containerd/containerd/issues/new/choose)
* Email us at [security@containerd.io] (mailto:security@containerd.io)
To report a security issue in containerd:
* [Report a new vulnerability] (https://github.com/containerd/containerd/security/advisories/new)</td><td></td><td></td><td></td><td></td></tr>
<tr><td>CVE-2025-61730</td><td>During the TLS 1.3 handshake if multiple messages are sent in records that span encryption level boundaries (for instance the Client Hello and Encrypted Extensions messages), the subsequent messages may be processed before the encryption level changes. This can cause some minor information disclosure if a network-local attacker can inject messages during the handshake.</td><td>V2: 4
V3: 4</td><td>go:stdlib<table><tr><th>Impacted Version</th><th>Fixed Version</th></tr><tr><td>1.24.5</td><td>>=1.24.12;>=1.25.6</td></tr><tr><td>1.25.0</td><td>>=1.24.12;>=1.25.6</td></tr><tr><td>1.24.4</td><td>>=1.24.12;>=1.25.6</td></tr><tr><td colspan="2">...(6 versions)</td></tr></table></td><td>Jan 29, 2026 01:46:09</td><td>Containers
argocd-application-controller-0
argocd-notifications-controller-7cf65d89f6-cqwj2
argocd-server-6c66b766f5-6f9vv
argocd-applicationset-controller-6d68c66d6d-wdxlg
argocd-repo-server-77977bc6f9-22bck
...(6 containers)
Images
quay.io/argoproj/argocd:v3.2.5
ghcr.io/dexidp/dex:v2.44.0</td></tr>
</table>

<table>
<tr><th>Name</th><th>Description</th><th>Score</th><th>Packages</th><th>Published at</th><th>Impact</th></tr>
<tr>
<td>CVE-2025-61729</td>
<td>Within HostnameError.Error(), when constructing an error string, there is no limit to the number of hosts that will be printed out. Furthermore, the error string is constructed by repeated string concatenation, leading to quadratic runtime. Therefore, a certificate provided by a malicious actor can result in excessive resource consumption.</td>
<td>V2: 7
V3: 7.5</td>
<td>go:stdlib
<table>
<tr><th>Impacted Version</th><th>Fixed Version</th></tr>
<tr><td>1.24.4</td><td>>=1.24.11;>=1.25.5</td></tr>
<tr><td>1.24.5</td><td>>=1.24.11;>=1.25.5</td></tr>
<tr><td>1.25.0</td><td>>=1.24.11;>=1.25.5</td></tr>
<tr><td colspan="2">...(5 versions)</td></tr>
</table>
</td>
<td>Dec 3, 2025
12:45:51</td>
<td>Containers
argocd-application-controller-0
argocd-notifications-controller-7cf65d89f6-cqwj2
argocd-server-6c66b766f5-6f9vv
argocd-applicationset-controller-6d68c66d6d-wdxlg
argocd-repo-server-77977bc6f9-22bck
...(6 containers)
Images
quay.io/argoproj/argocd:v3.2.5
ghcr.io/dexidp/dex:v2.44.0</td>
</tr>
<tr>
<td>CVE-2025-61728</td>
<td>archive/zip uses a super-linear file name indexing algorithm that is invoked the first time a file in an archive is opened. This can lead to a denial of service when consuming a maliciously constructed ZIP archive.</td>
<td>V2: 4
V3: 4</td>
<td>go:stdlib
<table>
<tr><th>Impacted Version</th><th>Fixed Version</th></tr>
<tr><td>1.22.7</td><td>>=1.24.12;>=1.25.6</td></tr>
<tr><td>1.23.5</td><td>>=1.24.12;>=1.25.6</td></tr>
<tr><td>1.25.5</td><td>>=1.24.12;>=1.25.6</td></tr>
<tr><td colspan="2">...(6 versions)</td></tr>
</table>
</td>
<td>Jan 29, 2026
01:46:09</td>
<td>Containers
argocd-application-controller-0
argocd-notifications-controller-7cf65d89f6-cqwj2
argocd-server-6c66b766f5-6f9vv
argocd-applicationset-controller-6d68c66d6d-wdxlg
argocd-repo-server-77977bc6f9-22bck
...(6 containers)
Images
quay.io/argoproj/argocd:v3.2.5
ghcr.io/dexidp/dex:v2.44.0</td>
</tr>
</table>

<table>
<tr><th>Name</th><th>Description</th><th>Score</th><th>Packages</th><th>Published at</th><th>Impact</th></tr>
<tr>
<td>CVE-2025-61727</td>
<td>An excluded subdomain constraint in a certificate chain does not restrict the usage of wildcard SANs in the leaf certificate. For example a constraint that excludes the subdomain test.example.com does not prevent a leaf certificate from claiming the SAN *.example.com.</td>
<td>V2: 4
V3: 6.5</td>
<td>go:stdlib
<table>
<tr><th>Impacted Version</th><th>Fixed Version</th></tr>
<tr><td>1.25.0</td><td>>=1.24.11;>=1.25.5</td></tr>
<tr><td>1.24.5</td><td>>=1.24.11;>=1.25.5</td></tr>
<tr><td>1.23.5</td><td>>=1.24.11;>=1.25.5</td></tr>
<tr><td colspan="2">...(5 versions)</td></tr>
</table>
</td>
<td>Dec 4, 2025
01:46:25</td>
<td>Containers
argocd-application-controller-0
argocd-notifications-controller-7cf65d89f6-cqwj2
argocd-server-6c66b766f5-6f9vv
argocd-applicationset-controller-6d68c66d6d-wdxlg
argocd-repo-server-77977bc6f9-22bck
...(6 containers)
Images
quay.io/argoproj/argocd:v3.2.5
ghcr.io/dexidp/dex:v2.44.0</td>
</tr>
<tr>
<td>CVE-2025-61726</td>
<td>The net/url package does not set a limit on the number of query parameters in a query.
While the maximum size of query parameters in URLs is generally limited by the maximum request header size, the net/http.Request.ParseForm method can parse large URL-encoded forms. Parsing a large form containing many unique query parameters can cause excessive memory consumption.</td>
<td>V2: 4
V3: 4</td>
<td>go:stdlib
<table>
<tr><th>Impacted Version</th><th>Fixed Version</th></tr>
<tr><td>1.25.0</td><td>>=1.24.12;>=1.25.6</td></tr>
<tr><td>1.24.5</td><td>>=1.24.12;>=1.25.6</td></tr>
<tr><td>1.22.7</td><td>>=1.24.12;>=1.25.6</td></tr>
<tr><td colspan="2">...(6 versions)</td></tr>
</table>
</td>
<td>Jan 29, 2026
01:46:09</td>
<td>Containers
argocd-application-controller-0
argocd-notifications-controller-7cf65d89f6-cqwj2
argocd-server-6c66b766f5-6f9vv
argocd-applicationset-controller-6d68c66d6d-wdxlg
argocd-repo-server-77977bc6f9-22bck
...(6 containers)
Images
quay.io/argoproj/argocd:v3.2.5
ghcr.io/dexidp/dex:v2.44.0</td>
</tr>
</table>

<table>
<tr><th>Name</th><th>Description</th><th>Score</th><th>Packages</th><th>Published at</th><th>Impact</th></tr>
<tr>
<td>CVE-2025-61725</td>
<td>The ParseAddress function constructs domain-literal address components through repeated string concatenation. When parsing large domain-literal components, this can cause excessive CPU consumption.</td>
<td>V2: 7
V3: 7.5</td>
<td>go:stdlib
<table>
<tr><th>Impacted Version</th><th>Fixed Version</th></tr>
<tr><td>1.24.5</td><td>>=1.24.8;>=1.25.2</td></tr>
<tr><td>1.25.0</td><td>>=1.24.8;>=1.25.2</td></tr>
<tr><td>1.24.4</td><td>>=1.24.8;>=1.25.2</td></tr>
<tr><td colspan="2">...(5 versions)</td></tr>
</table>
</td>
<td>Oct 30, 2025
04:46:20</td>
<td>Containers
argocd-application-controller-0
argocd-notifications-controller-7cf65d89f6-cqwj2
argocd-server-6c66b766f5-6f9vv
argocd-applicationset-controller-6d68c66d6d-wdxlg
argocd-repo-server-77977bc6f9-22bck
...(6 containers)

Images
quay.io/argoproj/argocd:v3.2.5
ghcr.io/dexidp/dex:v2.44.0</td>
</tr>
<tr>
<td>CVE-2025-61724</td>
<td>The Reader.ReadResponse function constructs a response string through repeated string concatenation of lines. When the number of lines in a response is large, this can cause excessive CPU consumption.</td>
<td>V2: 4
V3: 5.3</td>
<td>go:stdlib
<table>
<tr><th>Impacted Version</th><th>Fixed Version</th></tr>
<tr><td>1.25.0</td><td>>=1.24.8;>=1.25.2</td></tr>
<tr><td>1.24.5</td><td>>=1.24.8;>=1.25.2</td></tr>
<tr><td>1.24.4</td><td>>=1.24.8;>=1.25.2</td></tr>
<tr><td colspan="2">...(5 versions)</td></tr>
</table>
</td>
<td>Oct 30, 2025
04:46:20</td>
<td>Containers
argocd-application-controller-0
argocd-notifications-controller-7cf65d89f6-cqwj2
argocd-server-6c66b766f5-6f9vv
argocd-applicationset-controller-6d68c66d6d-wdxlg
argocd-repo-server-77977bc6f9-22bck
...(6 containers)

Images
quay.io/argoproj/argocd:v3.2.5
ghcr.io/dexidp/dex:v2.44.0</td>
</tr>
</table>

<table>
<tr><th>Name</th><th>Description</th><th>Score</th><th>Packages</th><th>Published at</th><th>Impact</th></tr>
<tr>
<td>CVE-2025-61723</td>
<td>The processing time for parsing some invalid inputs scales non-linearly with respect to the size of the input.
This affects programs which parse untrusted PEM inputs.</td>
<td>V2: 7
V3: 7.5</td>
<td>go:stdlib<table><tr><th>Impacted Version</th><th>Fixed Version</th></tr><tr><td>1.25.0</td><td>>=1.24.8;>=1.25.2</td></tr><tr><td>1.24.5</td><td>>=1.24.8;>=1.25.2</td></tr><tr><td>1.23.5</td><td>>=1.24.8;>=1.25.2</td></tr><tr><td colspan="2">...(5 versions)</td></tr></table></td>
<td>Oct 30, 2025
04:46:19</td>
<td>Containers
argocd-application-controller-0
argocd-notifications-controller-7cf65d89f6-cqwj2
argocd-server-6c66b766f5-6f9vv
argocd-applicationset-controller-6d68c66d6d-wdxlg
argocd-repo-server-77977bc6f9-22bck
...(6 containers)
Images
quay.io/argoproj/argocd:v3.2.5
ghcr.io/dexidp/dex:v2.44.0</td>
</tr>
<tr>
<td>CVE-2025-58189</td>
<td>When Conn.Handshake fails during ALPN negotiation the error contains attacker controlled information (the ALPN protocols sent by the client) which is not escaped.</td>
<td>V2: 4
V3: 5.3</td>
<td>go:stdlib<table><tr><th>Impacted Version</th><th>Fixed Version</th></tr><tr><td>1.23.5</td><td>>=1.24.8;>=1.25.2</td></tr><tr><td>1.25.0</td><td>>=1.24.8;>=1.25.2</td></tr><tr><td>1.24.5</td><td>>=1.24.8;>=1.25.2</td></tr><tr><td colspan="2">...(5 versions)</td></tr></table></td>
<td>Oct 30, 2025
04:46:19</td>
<td>Containers
argocd-application-controller-0
argocd-notifications-controller-7cf65d89f6-cqwj2
argocd-server-6c66b766f5-6f9vv
argocd-applicationset-controller-6d68c66d6d-wdxlg
argocd-repo-server-77977bc6f9-22bck
...(6 containers)
Images
quay.io/argoproj/argocd:v3.2.5
ghcr.io/dexidp/dex:v2.44.0</td>
</tr>
</table>

<table>
<tr><th>Name</th><th>Description</th><th>Score</th><th>Packages</th><th>Published at</th><th>Impact</th></tr>
<tr>
<td>CVE-2025-58188</td>
<td>Validating certificate chains which contain DSA public keys can cause programs to panic, due to a interface cast that assumes they implement the Equal method. This affects programs which validate arbitrary certificate chains.</td>
<td>V2: 7
V3: 7.5</td>
<td>go:stdlib
<table>
<tr><th>Impacted Version</th><th>Fixed Version</th></tr>
<tr><td>1.22.7</td><td>>=1.24.8;>=1.25.2</td></tr>
<tr><td>1.23.5</td><td>>=1.24.8;>=1.25.2</td></tr>
<tr><td>1.25.0</td><td>>=1.24.8;>=1.25.2</td></tr>
<tr><td colspan="2">...(5 versions)</td></tr>
</table>
</td>
<td>Oct 30, 2025
04:46:19</td>
<td>Containers
argocd-application-controller-0
argocd-notifications-controller-7cf65d89f6-cqwj2
argocd-server-6c66b766f5-6f9vv
argocd-applicationset-controller-6d68c66d6d-wdxlg
argocd-repo-server-77977bc6f9-22bck
...(6 containers)
Images
quay.io/argoproj/argocd:v3.2.5
ghcr.io/dexidp/dex:v2.44.0</td>
</tr>
<tr>
<td>CVE-2025-58187</td>
<td>Due to the design of the name constraint checking algorithm, the processing time of some inputs scale non-linearly with respect to the size of the certificate. This affects programs which validate arbitrary certificate chains.</td>
<td>V2: 7
V3: 7.5</td>
<td>go:stdlib
<table>
<tr><th>Impacted Version</th><th>Fixed Version</th></tr>
<tr><td>1.23.5</td><td>>=1.24.9;>=1.25.3</td></tr>
<tr><td>1.25.0</td><td>>=1.24.9;>=1.25.3</td></tr>
<tr><td>1.24.5</td><td>>=1.24.9;>=1.25.3</td></tr>
<tr><td colspan="2">...(5 versions)</td></tr>
</table>
</td>
<td>Oct 30, 2025
04:46:19</td>
<td>Containers
argocd-application-controller-0
argocd-notifications-controller-7cf65d89f6-cqwj2
argocd-server-6c66b766f5-6f9vv
argocd-applicationset-controller-6d68c66d6d-wdxlg
argocd-repo-server-77977bc6f9-22bck
...(6 containers)
Images
quay.io/argoproj/argocd:v3.2.5
ghcr.io/dexidp/dex:v2.44.0</td>
</tr>
</table>

<table>
<tr><th>Name</th><th>Description</th><th>Score</th><th>Packages</th><th>Published at</th><th>Impact</th></tr>
<tr>
<td>CVE-2025-58186</td>
<td>Despite HTTP headers having a default limit of 1MB, the number of cookies that can be parsed does not have a limit. By sending a lot of very small cookies such as "a=;", an attacker can make an HTTP server allocate a large amount of structs, causing large memory consumption.</td>
<td>V2: 4
V3: 5.3</td>
<td>go:stdlib
<table>
<tr><th>Impacted Version</th><th>Fixed Version</th></tr>
<tr><td>1.25.0</td><td>>=1.24.8;>=1.25.2</td></tr>
<tr><td>1.24.5</td><td>>=1.24.8;>=1.25.2</td></tr>
<tr><td>1.22.7</td><td>>=1.24.8;>=1.25.2</td></tr>
<tr><td colspan="2">...(5 versions)</td></tr>
</table>
</td>
<td>Oct 30, 2025
04:46:19</td>
<td>Containers
argocd-application-controller-0
argocd-notifications-controller-7cf65d89f6-cqwj2
argocd-server-6c66b766f5-6f9vv
argocd-applicationset-controller-6d68c66d6d-wdxlg
argocd-repo-server-77977bc6f9-22bck
...(6 containers)
Images
quay.io/argoproj/argocd:v3.2.5
ghcr.io/dexidp/dex:v2.44.0</td>
</tr>
<tr>
<td>CVE-2025-58185</td>
<td>Parsing a maliciously crafted DER payload could allocate large amounts of memory, causing memory exhaustion.</td>
<td>V2: 4
V3: 5.3</td>
<td>go:stdlib
<table>
<tr><th>Impacted Version</th><th>Fixed Version</th></tr>
<tr><td>1.24.4</td><td>>=1.24.8;>=1.25.2</td></tr>
<tr><td>1.24.5</td><td>>=1.24.8;>=1.25.2</td></tr>
<tr><td>1.25.0</td><td>>=1.24.8;>=1.25.2</td></tr>
<tr><td colspan="2">...(5 versions)</td></tr>
</table>
</td>
<td>Oct 30, 2025
04:46:19</td>
<td>Containers
argocd-application-controller-0
argocd-notifications-controller-7cf65d89f6-cqwj2
argocd-server-6c66b766f5-6f9vv
argocd-applicationset-controller-6d68c66d6d-wdxlg
argocd-repo-server-77977bc6f9-22bck
...(6 containers)
Images
quay.io/argoproj/argocd:v3.2.5
ghcr.io/dexidp/dex:v2.44.0</td>
</tr>
</table>

<table>
<tr><th>Name</th><th>Description</th><th>Score</th><th>Packages</th><th>Published at</th><th>Impact</th></tr>
<tr>
<td>CVE-2025-58183</td>
<td>tar.Reader does not set a maximum size on the number of sparse region data blocks in GNU tar pax 1.0 sparse files. A maliciously-crafted archive containing a large number of sparse regions can cause a Reader to read an unbounded amount of data from the archive into memory. When reading from a compressed source, a small compressed input can result in large allocations.</td>
<td>V2: 4
V3: 4.3</td>
<td>go:stdlib
<table>
<tr><th>Impacted Version</th><th>Fixed Version</th></tr>
<tr><td>1.25.0</td><td>>=1.24.8;>=1.25.2</td></tr>
<tr><td>1.24.5</td><td>>=1.24.8;>=1.25.2</td></tr>
<tr><td>1.23.5</td><td>>=1.24.8;>=1.25.2</td></tr>
<tr><td colspan="2">...(5 versions)</td></tr>
</table>
</td>
<td>Oct 30, 2025
04:46:19</td>
<td>Containers
argocd-application-controller-0
argocd-notifications-controller-7cf65d89f6-cqwj2
argocd-server-6c66b766f5-6f9vv
argocd-applicationset-controller-6d68c66d6d-wdxlg
argocd-repo-server-77977bc6f9-22bck
...(6 containers)
Images
quay.io/argoproj/argocd:v3.2.5
ghcr.io/dexidp/dex:v2.44.0</td>
</tr>
<tr>
<td>CVE-2025-58181</td>
<td>golang.org/x/crypto/ssh allows an attacker to cause unbounded memory consumption
SSH servers parsing GSSAPI authentication requests do not validate the number of mechanisms specified in the request, allowing an attacker to cause unbounded memory consumption.</td>
<td>V2: 4
V3: 5.3</td>
<td>go:golang.org/x/crypto
<table>
<tr><th>Impacted Version</th><th>Fixed Version</th></tr>
<tr><td>0.41.0</td><td>0.45.0</td></tr>
<tr><td>0.40.0</td><td>0.45.0</td></tr>
<tr><td>0.39.0</td><td>0.45.0</td></tr>
</table>
</td>
<td>Nov 20, 2025
04:31:20</td>
<td>Containers
argocd-application-controller-0
argocd-notifications-controller-7cf65d89f6-cqwj2
argocd-server-6c66b766f5-6f9vv
argocd-applicationset-controller-6d68c66d6d-wdxlg
argocd-repo-server-77977bc6f9-22bck
...(6 containers)
Images
quay.io/argoproj/argocd:v3.2.5
ghcr.io/dexidp/dex:v2.44.0</td>
</tr>
</table>

<table>
<tr><th>Name</th><th>Description</th><th>Score</th><th>Packages</th><th>Published at</th><th>Impact</th></tr>
<tr>
<td>CVE-2025-47914</td>
<td>golang.org/x/crypto/ssh/agent vulnerable to panic if message is malformed due to out of bounds read
SSH Agent servers do not validate the size of messages when processing new identity requests, which may cause the program to panic if the message is malformed due to an out of bounds read.</td>
<td>V2: 4
V3: 5.3</td>
<td>go:golang.org/x/crypto
<table>
<tr><th>Impacted Version</th><th>Fixed Version</th></tr>
<tr><td>0.40.0</td><td>0.45.0</td></tr>
<tr><td>0.41.0</td><td>0.45.0</td></tr>
<tr><td>0.39.0</td><td>0.45.0</td></tr>
</table>
</td>
<td>Nov 20, 2025
04:46:40</td>
<td>Containers
argocd-application-controller-0
argocd-notifications-controller-7cf65d89f6-cqwj2
argocd-server-6c66b766f5-6f9vv
argocd-applicationset-controller-6d68c66d6d-wdxlg
argocd-repo-server-77977bc6f9-22bck
...(6 containers)
Images
quay.io/argoproj/argocd:v3.2.5
ghcr.io/dexidp/dex:v2.44.0</td>
</tr>
<tr>
<td>CVE-2025-47913</td>
<td>SSH clients receiving SSH_AGENT_SUCCESS when expecting a typed response will panic and cause early termination of the client process.</td>
<td>V2: 7
V3: 7.5</td>
<td>go:golang.org/x/crypto
<table>
<tr><th>Impacted Version</th><th>Fixed Version</th></tr>
<tr><td>0.40.0</td><td>>=0.43.0</td></tr>
<tr><td>0.41.0</td><td>>=0.43.0</td></tr>
<tr><td>0.39.0</td><td>>=0.43.0</td></tr>
</table>
</td>
<td>Nov 14, 2025
03:45:51</td>
<td>Containers
argocd-application-controller-0
argocd-notifications-controller-7cf65d89f6-cqwj2
argocd-server-6c66b766f5-6f9vv
argocd-applicationset-controller-6d68c66d6d-wdxlg
argocd-repo-server-77977bc6f9-22bck
...(6 containers)
Images
quay.io/argoproj/argocd:v3.2.5
ghcr.io/dexidp/dex:v2.44.0</td>
</tr>
</table>

Name	Description	Score	Packages	Published at	Impact
CVE-2025-47912	The Parse function permits values other than IPv6 addresses to be included in square brackets within the host component of a URL. RFC 3986 permits IPv6 addresses to be included within the host component, enclosed within square brackets. For example: "http://[::1]/". IPv4 addresses and hostnames must not appear within square brackets. Parse did not enforce this requirement.	V2: 4 V3: 5.3	go:stdlib Impacted Version / Fixed Version 1.24.4 / >=1.24.8;>=1.25.2 1.22.7 / >=1.24.8;>=1.25.2 1.23.5 / >=1.24.8;>=1.25.2 ...(5 versions)	Oct 30, 2025 04:46:18	**Containers** argocd-application-controller-0 argocd-notifications-controller-7cf65d89f6-cqwj2 argocd-server-6c66b766f5-6f9vv argocd-applicationset-controller-6d68c66d6d-wdxlg argocd-repo-server-77977bc6f9-22bck ...(6 containers) **Images** quay.io/argoproj/argocd:v3.2.5 ghcr.io/dexidp/dex:v2.44.0
CVE-2025-47910	When using http.CrossOriginProtection, the AddInsecureBypassPattern method can unexpectedly bypass more requests than intended. CrossOriginProtection then skips validation, but forwards the original request path, which may be served by a different handler without the intended security protections.	V2: 4 V3: 5.4	go:stdlib Impacted Version / Fixed Version 1.25.0 / >=1.25.1	Sep 23, 2025 02:45:59	**Containers** argocd-dex-server-88bbf995c-92jj7 **Images** ghcr.io/dexidp/dex:v2.44.0
CVE-2025-47907	Cancelling a query (e.g. by cancelling the context passed to one of the query methods) during a call to the Scan method of the returned Rows can result in unexpected results if other queries are being made in parallel. This can result in a race condition that may overwrite the expected results with those of another query, causing the call to Scan to return either unexpected results from the other query or an error.	V2: 7 V3: 7	go:stdlib Impacted Version / Fixed Version 1.24.5 / >=1.23.12;>=1.24.6 1.23.5 / >=1.23.12;>=1.24.6 1.22.7 / >=1.23.12;>=1.24.6 ...(4 versions)	Aug 7, 2025 09:45:30	**Containers** argocd-application-controller-0 argocd-notifications-controller-7cf65d89f6-cqwj2 argocd-server-6c66b766f5-6f9vv argocd-applicationset-controller-6d68c66d6d-wdxlg argocd-repo-server-77977bc6f9-22bck ...(6 containers) **Images** quay.io/argoproj/argocd:v3.2.5 ghcr.io/dexidp/dex:v2.44.0

Name	Description	Score	Packages	Published at	Impact
CVE-2025-47906	If the PATH environment variable contains paths which are executables (rather than just directories), passing certain strings to LookPath ("", ".", and ".."), can result in the binaries listed in the PATH being unexpectedly returned.	V2: 4 V3: 6.5	go:stdlib Impacted Version / Fixed Version 1.24.5 / >=1.23.12;>=1.24.6 1.23.5 / >=1.23.12;>=1.24.6 1.22.7 / >=1.23.12;>=1.24.6 ...(4 versions)	Sep 19, 2025 12:45:37	**Containers** argocd-application-controller-0 argocd-notifications-controller-7cf65d89f6-cqwj2 argocd-server-6c66b766f5-6f9vv argocd-applicationset-controller-6d68c66d6d-wdxlg argocd-repo-server-77977bc6f9-22bck ...(6 containers) **Images** quay.io/argoproj/argocd:v3.2.5 ghcr.io/dexidp/dex:v2.44.0
CVE-2025-4673	Proxy-Authorization and Proxy-Authenticate headers persisted on cross-origin redirects potentially leaking sensitive information.	V2: 4 V3: 6.8	go:stdlib Impacted Version / Fixed Version 1.23.5 / >=1.23.10;>=1.24.4 1.22.7 / >=1.23.10;>=1.24.4	Jun 11, 2025 10:45:42	**Containers** argocd-application-controller-0 argocd-notifications-controller-7cf65d89f6-cqwj2 argocd-server-6c66b766f5-6f9vv argocd-applicationset-controller-6d68c66d6d-wdxlg argocd-repo-server-77977bc6f9-22bck **Images** quay.io/argoproj/argocd:v3.2.5
CVE-2025-46394	In tar in BusyBox through 1.37.0, a TAR archive can have filenames hidden from a listing through the use of terminal escape sequences.	V2: 1 V3: 3.2	busybox Impacted Version / Fixed Version 1.37.0-r18 / 1.37.0-r20 1.37.0-r19 / 1.37.0-r20	Apr 23, 2025 09:45:48	**Containers** argocd-redis-7fd4c97dd4-d4fr8 argocd-dex-server-88bbf995c-92jj7 **Images** ecr-public.aws.com/docker/library/redis:8.2.2-alpine ghcr.io/dexidp/dex:v2.44.0

<table>
<tr><th>Name</th><th>Description</th><th>Score</th><th>Packages</th><th>Published at</th><th>Impact</th></tr>
<tr>
<td>CVE-2025-22871</td>
<td>The net/http package improperly accepts a bare LF as a line terminator in chunked data chunk-size lines. This can permit request smuggling if a net/http server is used in conjunction with a server that incorrectly accepts a bare LF as part of a chunk-ext.</td>
<td>V2: 9
V3: 9.1</td>
<td>go:stdlib
<table>
<tr><th>Impacted Version</th><th>Fixed Version</th></tr>
<tr><td>1.23.5</td><td>>=1.23.8;>=1.24.2</td></tr>
<tr><td>1.22.7</td><td>>=1.23.8;>=1.24.2</td></tr>
</table>
</td>
<td>Apr 9, 2025
01:45:20</td>
<td>Containers
argocd-application-controller-0
argocd-notifications-controller-7cf65d89f6-cqwj2
argocd-server-6c66b766f5-6f9vv
argocd-applicationset-controller-6d68c66d6d-wdxlg
argocd-repo-server-77977bc6f9-22bck
Images
quay.io/argoproj/argocd:v3.2.5</td>
</tr>
<tr>
<td>CVE-2025-22866</td>
<td>Due to the usage of a variable time instruction in the assembly implementation of an internal function, a small number of bits of secret scalars are leaked on the ppc64le architecture. Due to the way this function is used, we do not believe this leakage is enough to allow recovery of the private key when P-256 is used in any well known protocols.</td>
<td>V2: 4
V3: 4</td>
<td>go:stdlib
<table>
<tr><th>Impacted Version</th><th>Fixed Version</th></tr>
<tr><td>1.23.5</td><td>>=1.22.12;>=1.23.6;>=1.24.0-rc.3</td></tr>
<tr><td>1.22.7</td><td>>=1.22.12;>=1.23.6;>=1.24.0-rc.3</td></tr>
</table>
</td>
<td>Feb 6, 2025
10:45:21</td>
<td>Containers
argocd-application-controller-0
argocd-notifications-controller-7cf65d89f6-cqwj2
argocd-server-6c66b766f5-6f9vv
argocd-applicationset-controller-6d68c66d6d-wdxlg
argocd-repo-server-77977bc6f9-22bck
Images
quay.io/argoproj/argocd:v3.2.5</td>
</tr>
</table>

Name	Description	Score	Packages	Published at	Impact
CVE-2025-15469	Issue summary: The 'openssl dgst' command-line tool silently truncates input data to 16MB when using one-shot signing algorithms and reports success instead of an error. Impact summary: A user signing or verifying files larger than 16MB with one-shot algorithms (such as Ed25519, Ed448, or ML-DSA) may believe the entire file is authenticated while trailing data beyond 16MB remains unauthenticated. When the 'openssl dgst' command is used with algorithms that only support one-shot signing (Ed25519, Ed448, ML-DSA-44, ML-DSA-65, ML-DSA-87), the input is buffered with a 16MB limit. If the input exceeds this limit, the tool silently truncates to the first 16MB and continues without signaling an error, contrary to what the documentation states. This creates an integrity gap where trailing bytes can be modified without detection if both signing and verification are performed using the same affected codepath. The issue affects only the command-line tool behavior. Verifiers that process the full message using library APIs will reject the signature, so the risk primarily affects workflows that both sign and verify with the affected 'openssl dgst' command. Streaming digest algorithms for 'openssl dgst' and library users are unaffected. The FIPS modules in 3.5 and 3.6 are not affected by this issue, as the	V2: 4 V3: 5.5	openssl Impacted Version / Fixed Version 3.5.1-r0 / 3.5.5-r0 3.5.4-r0 / 3.5.5-r0	Jan 27, 2026 09:46:14	**Containers** argocd-redis-7fd4c97dd4-d4fr8 argocd-dex-server-88bbf995c-92jj7 **Images** ecr-public.aws.com/docker/library/redis:8.2.2-alpine ghcr.io/dexidp/dex:v2.44.0

Name	Description	Score	Packages	Published at	Impact
	command-line tools are outside the OpenSSL FIPS module boundary. OpenSSL 3.5 and 3.6 are vulnerable to this issue. OpenSSL 3.4, 3.3, 3.0, 1.1.1 and 1.0.2 are not affected by this issue.				
CVE-2025-15468	Issue summary: If an application using the SSL_CIPHER_find() function in a QUIC protocol client or server receives an unknown cipher suite from the peer, a NULL dereference occurs. Impact summary: A NULL pointer dereference leads to abnormal termination of the running process causing Denial of Service. Some applications call SSL_CIPHER_find() from the client_hello_cb callback on the cipher ID received from the peer. If this is done with an SSL object implementing the QUIC protocol, NULL pointer dereference will happen if the examined cipher ID is unknown or unsupported. As it is not very common to call this function in applications using the QUIC protocol and the worst outcome is Denial of Service, the issue was assessed as Low severity. The vulnerable code was introduced in the 3.2 version with the addition of the QUIC protocol support. The FIPS modules in 3.6, 3.5, 3.4 and 3.3 are not affected by this issue, as the QUIC implementation is outside the OpenSSL FIPS module boundary. OpenSSL 3.6, 3.5, 3.4 and 3.3 are vulnerable to this issue. OpenSSL 3.0, 1.1.1 and 1.0.2 are not affected by this issue.	V2: 4 V3: 5.9	openssl Impacted Version / Fixed Version 3.5.1-r0 / 3.5.5-r0 3.5.4-r0 / 3.5.5-r0	Jan 27, 2026 09:46:14	**Containers** argocd-redis-7fd4c97dd4-d4fr8 argocd-dex-server-88bbf995c-92jj7 **Images** ecr-public.aws.com/docker/library/redis:8.2.2-alpine ghcr.io/dexidp/dex:v2.44.0

Name	Description	Score	Packages	Published at	Impact
CVE-2025-15467	Issue summary: Parsing CMS AuthEnvelopedData message with maliciously crafted AEAD parameters can trigger a stack buffer overflow. Impact summary: A stack buffer overflow may lead to a crash, causing Denial of Service, or potentially remote code execution. When parsing CMS AuthEnvelopedData structures that use AEAD ciphers such as AES-GCM, the IV (Initialization Vector) encoded in the ASN.1 parameters is copied into a fixed-size stack buffer without verifying that its length fits the destination. An attacker can supply a crafted CMS message with an oversized IV, causing a stack-based out-of-bounds write before any authentication or tag verification occurs. Applications and services that parse untrusted CMS or PKCS#7 content using AEAD ciphers (e.g., S/MIME AuthEnvelopedData with AES-GCM) are vulnerable. Because the overflow occurs prior to authentication, no valid key material is required to trigger it. While exploitability to remote code execution depends on platform and toolchain mitigations, the stack-based write primitive represents a severe risk. The FIPS modules in 3.6, 3.5, 3.4, 3.3 and 3.0 are not affected by this issue, as the CMS implementation is outside the OpenSSL FIPS module boundary. OpenSSL 3.6, 3.5, 3.4, 3.3 and 3.0 are vulnerable to this issue.	V2: 9 V3: 9.8	openssl Impacted Version / Fixed Version 3.5.1-r0 / 3.5.5-r0 3.5.4-r0 / 3.5.5-r0	Jan 27, 2026 09:46:14	**Containers** argocd-redis-7fd4c97dd4-d4fr8 argocd-dex-server-88bbf995c-92jj7 **Images** ecr-public.aws.com/docker/library/redis:8.2.2-alpine ghcr.io/dexidp/dex:v2.44.0

Name	Description	Score	Packages	Published at	Impact
	OpenSSL 1.1.1 and 1.0.2 are not affected by this issue.				

Name	Description	Score	Packages	Published at	Impact
CVE-2025-11187	Issue summary: PBMAC1 parameters in PKCS#12 files are missing validation which can trigger a stack-based buffer overflow, invalid pointer or NULL pointer dereference during MAC verification. Impact summary: The stack buffer overflow or NULL pointer dereference may cause a crash leading to Denial of Service for an application that parses untrusted PKCS#12 files. The buffer overflow may also potentially enable code execution depending on platform mitigations. When verifying a PKCS#12 file that uses PBMAC1 for the MAC, the PBKDF2 salt and keylength parameters from the file are used without validation. If the value of keylength exceeds the size of the fixed stack buffer used for the derived key (64 bytes), the key derivation will overflow the buffer. The overflow length is attacker-controlled. Also, if the salt parameter is not an OCTET STRING type this can lead to invalid or NULL pointer dereference. Exploiting this issue requires a user or application to process a maliciously crafted PKCS#12 file. It is uncommon to accept untrusted PKCS#12 files in applications as they are usually used to store private keys which are trusted by definition. For this reason the issue was assessed as Moderate severity. The FIPS modules in 3.6, 3.5 and 3.4 are not affected by this issue, as	V2: 4 V3: 6.1	openssl Impacted Version / Fixed Version 3.5.1-r0 / 3.5.5-r0 3.5.4-r0 / 3.5.5-r0	Jan 27, 2026 09:46:14	**Containers** argocd-redis-7fd4c97dd4-d4fr8 argocd-dex-server-88bbf995c-92jj7 **Images** ecr-public.aws.com/docker/library/redis:8.2.2-alpine ghcr.io/dexidp/dex:v2.44.0

<table>
<tr><th>Name</th><th>Description</th><th>Score</th><th>Packages</th><th>Published at</th><th>Impact</th></tr>
<tr><td></td><td>PKCS#12 processing is outside the OpenSSL FIPS module boundary.
OpenSSL 3.6, 3.5 and 3.4 are vulnerable to this issue.
OpenSSL 3.3, 3.0, 1.1.1 and 1.0.2 are not affected by this issue as they do
not support PBMAC1 in PKCS#12.</td><td></td><td></td><td></td><td></td></tr>
<tr><td>CVE-2025-0913</td><td>os.OpenFile(path, os.O_CREATE|O_EXCL) behaved differently on Unix and Windows systems when the target path was a dangling symlink. On Unix systems, OpenFile with O_CREATE and O_EXCL flags never follows symlinks. On Windows, when the target path was a symlink to a nonexistent location, OpenFile would create a file in that location. OpenFile now always returns an error when the O_CREATE and O_EXCL flags are both set and the target path is a symlink.</td><td>V2: 4
V3: 5.5</td><td>go:stdlib<table><tr><th>Impacted Version</th><th>Fixed Version</th></tr><tr><td>1.23.5</td><td>>=1.23.10;>=1.24.4</td></tr><tr><td>1.22.7</td><td>>=1.23.10;>=1.24.4</td></tr></table></td><td>Jun 11, 2025
11:45:24</td><td>Containers
argocd-application-controller-0
argocd-notifications-controller-7cf65d89f6-cqwj2
argocd-server-6c66b766f5-6f9vv
argocd-applicationset-controller-6d68c66d6d-wdxlg
argocd-repo-server-77977bc6f9-22bck
Images
quay.io/argoproj/argocd:v3.2.5</td></tr>
<tr><td>CVE-2024-7598</td><td>Kubernetes kube-apiserver Vulnerable to Race Condition in k8s.io/kubernetes</td><td>V2: 1
V3: 3.1</td><td>go:k8s.io/kubernetes<table><tr><th>Impacted Version</th><th>Fixed Version</th></tr><tr><td>1.34.2</td><td>N/A</td></tr></table></td><td>Mar 20, 2025
10:45:37</td><td>Containers
argocd-application-controller-0
argocd-notifications-controller-7cf65d89f6-cqwj2
argocd-server-6c66b766f5-6f9vv
argocd-applicationset-controller-6d68c66d6d-wdxlg
argocd-repo-server-77977bc6f9-22bck
Images
quay.io/argoproj/argocd:v3.2.5</td></tr>
</table>

Name	Description	Score	Packages	Published at	Impact
CVE-2024-58251	In netstat in BusyBox through 1.37.0, local users can launch of network application with an argv[0] containing an ANSI terminal escape sequence, leading to a denial of service (terminal locked up) when netstat is used by a victim.	V2: 1 V3: 2.5	busybox Impacted Version: 1.37.0-r18, Fixed Version: 1.37.0-r20 Impacted Version: 1.37.0-r19, Fixed Version: 1.37.0-r20	Apr 23, 2025 11:46:03	**Containers** argocd-redis-7fd4c97dd4-d4fr8 argocd-dex-server-88bbf995c-92jj7 **Images** ecr-public.aws.com/docker/library/redis:8.2.2-alpine ghcr.io/dexidp/dex:v2.44.0
CVE-2024-45341	A certificate with a URI which has a IPv6 address with a zone ID may incorrectly satisfy a URI name constraint that applies to the certificate chain. Certificates containing URIs are not permitted in the web PKI, so this only affects users of private PKIs which make use of URIs.	V2: 4 V3: 6.1	go:stdlib Impacted Version: 1.22.7, Fixed Version: >=1.22.11;>=1.23.5;>=1.24.0-rc.2	Jan 28, 2025 07:45:29	**Containers** argocd-application-controller-0 argocd-notifications-controller-7cf65d89f6-cqwj2 argocd-server-6c66b766f5-6f9vv argocd-applicationset-controller-6d68c66d6d-wdxlg argocd-repo-server-77977bc6f9-22bck **Images** quay.io/argoproj/argocd:v3.2.5
CVE-2024-45336	The HTTP client drops sensitive headers after following a cross-domain redirect. For example, a request to a.com/ containing an Authorization header which is redirected to b.com/ will not send that header to b.com. In the event that the client received a subsequent same-domain redirect, however, the sensitive headers would be restored. For example, a chain of redirects from a.com/, to b.com/1, and finally to b.com/2 would incorrectly send the Authorization header to b.com/2.	V2: 4 V3: 6.1	go:stdlib Impacted Version: 1.22.7, Fixed Version: >=1.22.11;>=1.23.5;>=1.24.0-rc.2	Jan 28, 2025 07:45:28	**Containers** argocd-application-controller-0 argocd-notifications-controller-7cf65d89f6-cqwj2 argocd-server-6c66b766f5-6f9vv argocd-applicationset-controller-6d68c66d6d-wdxlg argocd-repo-server-77977bc6f9-22bck **Images** quay.io/argoproj/argocd:v3.2.5

Name	Description	Score	Packages	Published at	Impact
CVE-2024-25621	containerd affected by a local privilege escalation via wide permissions on CRI directory ### Impact An overly broad default permission vulnerability was found in containerd. - `/var/lib/containerd` was created with the permission bits 0o711, while it should be created with 0o700 - Allowed local users on the host to potentially access the metadata store and the content store - `/run/containerd/io.containerd.grpc.v1.cri` was created with 0o755, while it should be created with 0o700 - Allowed local users on the host to potentially access the contents of Kubernetes local volumes. The contents of volumes might include setuid binaries, which could allow a local user on the host to elevate privileges on the host. - `/run/containerd/io.containerd.sandbox.controller.v1.shim` was created with 0o711, while it should be created with 0o700 The directory paths may differ depending on the daemon configuration. When the `temp` directory path is specified in the daemon configuration, that directory was also created with 0o711, while it should be created with 0o700. ### Patches This bug has been fixed in the following containerd versions: * 2.2.0 * 2.1.5 * 2.0.7 * 1.7.29	V2: 7 V3: 7.3	go:github.com/containerd/containerd Impacted Version: 1.7.27 Fixed Version: 1.7.29	Nov 6, 2025 08:42:08	**Containers** argocd-application-controller-0 argocd-notifications-controller-7cf65d89f6-cqwj2 argocd-server-6c66b766f5-6f9vv argocd-applicationset-controller-6d68c66d6d-wdxlg argocd-repo-server-77977bc6f9-22bck **Images** quay.io/argoproj/argocd:v3.2.5

Name	Description	Score	Packages	Published at	Impact
	Users should update to these versions to resolve the issue. These updates automatically change the permissions of the existing directories. > [!NOTE] > > `/run/containerd` and `/run/containerd/io.containerd.runtime.v2.task` are still created with 0o711. > This is an expected behavior for supporting userns-remapped containers. ### Workarounds The system administrator on the host can manually chmod the directories to not have group or world accessible permisisons: ``` chmod 700 /var/lib/containerd chmod 700 /run/containerd/io.containerd.grpc.v1.cri chmod 700 /run/containerd/io.containerd.sandbox.controller.v1.shim ``` An alternative mitigation would be to run containerd in [rootless mode](https://github.com/containerd/containerd/blob/main/docs/rootless.md). ### Credits The containerd project would like to thank David Leadbeater for responsibly disclosing this issue in accordance with the [containerd security policy](https://github.com/containerd/project/blob/main/SECURITY.md). ### For more information If you have any questions or comments about this advisory:				

Name	Description	Score	Packages	Published at	Impact
	* Open an issue in [containerd] (https://github.com/containerd/containerd/issues/new/choose) * Email us at [security@containerd.io] (mailto:security@containerd.io) To report a security issue in containerd: * [Report a new vulnerability] (https://github.com/containerd/containerd/security/advisories/new)				