Daily brief, Friday, July 3, 2026

Jul 2, 8:00 PM to Jul 3, 8:00 PM ET

Generated Nov 4, 2026, 4:23 AM ET

0	0	0	27	0	1
Breaking	Newly exploited	Exploit code	Critical CVEs	Ransomware posts	New breaches

27 new critical CVEs, 1 new breaches.

Breaking

Nothing spreading fast in technology large companies run.

Newly exploited in the wild

No CVEs added to CISA's known-exploited list.

New public exploit code

No new Nuclei templates, Metasploit modules, Exploit-DB or VulnCheck XDB entries.

New critical CVEs

27

9.8 **CVE-2026-20896** Gitea Gitea Open Source Git Server EXPLOIT CODE DETECTION

Gitea Docker image versions up to and including 1.26.2 use REVERSE_PROXY_TRUSTED_PROXIES=* by default, allowing any source IP to impersonate a user when reverse-proxy authentication headers such as X-WEBAUTH-USER are enabled.

9.8 **CVE-2026-9079** Curl curl

Product not on watchlist.

9.8 **CVE-2026-11856** Curl curl

Product not on watchlist.

9.1 **CVE-2026-8927** Curl curl

Product not on watchlist.

9.8 **CVE-2026-10536** Haxx curl

A use-after-free vulnerability exists in libcurl when an application configures an HTTP/2 stream-dependency tree via `CURLOPT_STREAM_DEPENDS` or `CURLOPT_STREAM_DEPENDS_E`, subsequently invokes `curl_easy_reset()`, and finally terminates the handle with `curl_

9.8 **CVE-2026-8925** Haxx curl

The curl logic that works with SASL authentication could end up cleaning up the GSASL context *twice* without clearing the pointer in between, making it `free()` the same pointer twice.

9.1 **CVE-2026-11564** Haxx curl

libcurl keeps previously used connections in a connection pool for subsequent transfers to reuse if one of them matches the setup. An easy handle that first uses default native CA trust can continue trusting the native platform store after the application swit

9.1 **CVE-2026-8924** Haxx curl

A flaw in curl's cookie parsing logic allows a malicious HTTP server to set "super cookies" that bypass the Public Suffix List check. This enables an attacker-controlled origin to inject cookies that curl subsequently scopes and transmits to unrelated third-pa

9.1 **CVE-2026-8926** Haxx curl

When asking curl to use a `.netrc` file to find credentials and at the same time specifying a URL with a username (without a password), like `https://user@example.com/`, curl could wrongly get and use the password for *another* user set in the `.netrc` file fo

9.0 **CVE-2026-58289** Microsoft edge chromium

Access of resource using incompatible type ('type confusion') in Microsoft Edge (Chromium-based) allows an unauthorized attacker to execute code over a network.

9.8 **CVE-2026-12481** Keras keras

A vulnerability in keras-team/keras version 3.14.0 allows for arbitrary code execution due to improper handling of deserialization in the `Lambda` layer. Specifically, the `_raise_for_lambda_deserialization()` function fails to enforce the safe-mode guard when

9.8 **CVE-2026-26292** Gitea Gitea Open Source Git Server

Gitea versions before 1.25.5 do not use the migration HTTP transport for LFS push and sync mirror operations, bypassing the configured migration transport protections for those LFS requests.

9.8 **CVE-2026-27780** Gitea Gitea Open Source Git Server

Gitea versions before 1.26.0 do not fail closed on bufio.Scanner errors while processing pre-receive hook input, allowing oversized input to bypass branch-protection checks.

9.1 **CVE-2026-20706** Gitea Gitea Open Source Git Server

Gitea versions up to and including 1.26.1 allow repository archive downloads to bypass token scope checks on the web archive download endpoint.

9.1 **CVE-2026-25718** Gitea Gitea Open Source Git Server

Gitea versions before 1.25.5 mishandle path resolution during template repository generation, allowing template processing to read or write through symlinked or otherwise non-regular paths.

9.1 **CVE-2026-22547** Gitea Gitea Open Source Git Server

Gitea versions before 1.25.5 lack validation constraints for repository creation fields, including length-limited template fields and trust model or object format values.

9.1 **CVE-2026-26232** Gitea Gitea Open Source Git Server

Gitea versions before 1.25.5 do not consistently enforce OAuth2 authorization code expiry and single-use behavior during token exchange.

9.1 **CVE-2026-26247** Gitea Gitea Open Source Git Server

Gitea versions before 1.25.5 do not persist the OAuth2 PKCE S256 challenge method correctly during authorization, allowing token exchange without the expected verifier check.

9.6 **CVE-2026-22874** Gitea Gitea Open Source Git Server

Gitea versions up to and including 1.26.2 have incomplete SSRF protection in webhook and migration allow-list filtering.

10.0 **CVE-2026-13768**

Gardyn devices expose a privileged iothubowner key. Access to this key will allow a malicious user to invoke an IoTHub Registry Manager function which returns connection information for all Gardyn Home Kit and Studio devices. Access to this key also allows a m

7 more critical CVEs in this window: see the dashboard

Ransomware

No leak-site posts collected.

New data breaches 1

Moody Bible Institute moody.edu 2,303,416 accounts

Watch Floor collects CVE records, CISA KEV, exploit indexes, official advisories, security news and chatter. CVSS is the headline score. Ransomware posts are criminal groups' claims, not confirmed by the victims. CVE IDs link to the full record on Watch Floor.