Daily brief, Friday, July 24, 2026

Jul 23, 8:00 PM to Jul 24, 8:00 PM ET

Generated Nov 3, 2026, 9:25 AM ET

0	0	0	22	0	0
Breaking	Newly exploited	Exploit code	Critical CVEs	Ransomware posts	New breaches

22 new critical CVEs.

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

22

10.0 **CVE-2026-56191** Microsoft exchange online

Improper authentication in Microsoft Exchange Online allows an unauthorized attacker to perform tampering over a network.

10.0 **CVE-2026-58275** Microsoft azure dns

Missing authorization in Azure DNS allows an unauthorized attacker to elevate privileges over a network.

10.0 **CVE-2026-62825** Microsoft azure key vault

Improper authentication in Azure Key Vault allows an unauthorized attacker to elevate privileges over a network.

10.0 **CVE-2026-56163** Microsoft azure kubernetes service

Missing authentication for critical function in Microsoft Azure Kubernetes Service allows an unauthorized attacker to elevate privileges over a network.

10.0 **CVE-2026-58630** Microsoft azure app service for linux

Improper access control in Azure App Service allows an unauthorized attacker to elevate privileges over a network.

9.9 **CVE-2026-50517** Microsoft 365 copilot
Deserialization of untrusted data in M365 Copilot allows an authorized attacker to execute code over a network.

9.8 **CVE-2026-64216** Linux linux kernel
In the Linux kernel, the following vulnerability has been resolved: netfs: Fix potential UAF in netfs_unlock_abandoned_read_pages() netfs_unlock_abandoned_read_pages(rreq) accesses the index of the folios it is wanting to unlock and compares that to rreq->no_u

9.8 **CVE-2026-64232** Linux linux kernel
In the Linux kernel, the following vulnerability has been resolved: block: recompute nr_integrity_segments in blk_insert_cloned_request blk_insert_cloned_request() already recomputes nr_phys_segments against the bottom queue, because "the queue settings relate

9.3 **CVE-2026-62835** Microsoft azure portal
Improper authorization in Azure Portal allows an unauthorized attacker to disclose information over a network.

9.1 **CVE-2026-56160** Microsoft azure red hat openshift
Improper authorization in Azure Red Hat OpenShift (ARO) allows an authorized attacker to elevate privileges over a network.

10.0 **CVE-2026-57106** Microsoft purview data governance
Server-side request forgery (ssrf) in Data Quality allows an unauthorized attacker to elevate privileges over a network.

9.9 **CVE-2026-54120** Microsoft surface management services
Improper input validation in Microsoft Surface allows an authorized attacker to execute code over a network.

9.8 **CVE-2026-56165** Microsoft account
Heap-based buffer overflow in Microsoft Account allows an unauthorized attacker to execute code over a network.

9.8 **CVE-2026-15704**
In Eclipse BaSyx Go Components versions up to and including 1.0.0, ABAC-enabled deployments are vulnerable to an authorization bypass caused by inconsistent trailing-slash handling between the ABAC middleware and the HTTP router. The shared router configuratio

9.8 **CVE-2026-16634**
TOML::XS versions before 0.06 for Perl bundle an unsupported and vulnerable version of tomlc99. The tomlc99 library is no longer maintained, and has an uncontrolled recursion vulnerability publicly reported in the issue tracker. Any caller that passes untruste

9.8 **CVE-2026-58586**
Image::WebP versions before 0.3.0 for Perl bundle a vulnerable version of libwebp. Image::WebP does not link to the system libwebp. Instead, it uses a bundled copy of libwebp 0.3.0 (released 2013-03-20). That version has multiple known vulnerabilities, includi

9.8 **CVE-2026-61884**
The Tycon Systems TPDIN-Monitor-WEB2 ships without HTTP credentials configured, intended for an installer to set them on first use. On firmware 2.4.4 and earlier, a unit left in this unconfigured state serves the web management interface without requiring any

9.8 **CVE-2026-16280** Imaginationtech ddk

An integer overflow when calculating physical offsets for sparse PMRs may result in 32-bit truncation of address computations for PMRs larger than 4 GB. This can lead to incorrect GPU MMU mappings and may allow a non-privileged user to trigger access to uninte

9.3 **CVE-2026-24727**

An unrestricted upload of file with dangerous type vulnerability in the e-paper draft upload function of SUNNET Corporate Training Management System through v10.3 allows remote authenticated users with administrator privileges to execute arbitrary commands by

9.2 **CVE-2026-12503**

Improper Link Resolution (CWE-59) in `/usr/bin/larm_starter` in Loytec L-INX, L-GATE, L-ROC, L-IOB, L-DALI, L-VIS and L-PAD through 8.4.16 on LINX-A64 allows an authenticated `larmapp` attacker to make `/etc/passwd` writable by the `larmapp` group (leading to

2 more critical CVEs in this window: see the dashboard

Ransomware

No leak-site posts collected.

New data breaches

No new breaches published.

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.