Daily brief, Friday, August 21, 2026

Aug 20, 8:00 PM to Aug 21, 8:00 PM ET

Generated Nov 2, 2026, 6:29 AM ET

0	1	0	40	0	0
Breaking	Newly exploited	Exploit code	Critical CVEs	Ransomware posts	New breaches

1 newly exploited, 40 new critical CVEs.

Breaking

Nothing spreading fast in technology large companies run.

Newly exploited in the wild

1

8.9 **CVE-2026-73570** Synacor Zimbra Collaboration Suite (ZCS) CISA KEV DETECTION

An attacker executes arbitrary code on the Zimbra Collaboration Suite server.

New public exploit code

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

New critical CVEs

40

10.0 **CVE-2026-69502** Microsoft azure sql database

Server-side request forgery (ssrf) in Azure SQL Database allows an unauthorized attacker to elevate privileges over a network.

10.0 **CVE-2026-61539**

Xinference is an inference API for running open-source, speech, and multimodal models. In 2.5.0 and earlier, Xinference passes attacker-influenced Llama3 tool-call output to eval() in xinference/model/llm/tool_parsers/llama3_tool_parser.py and xinference/model

9.9 **CVE-2026-77683** DETECTION

A security flaw has been discovered in Comfast CF-N1-S 2.6.0.1. Affected by this issue is the function system of the file /cgi-bin/mbox-config?method=SET&section=ntp_timezone. The manipulation of the argument timestr results in command injection. The attack ca

9.9 **CVE-2026-48749**

Incus is a system container and virtual machine manager. Prior to version 7.2.0, a specially crafted image can be used to read or create/write arbitrary files on the host; possibly leading to arbitrary command execution. Version 7.2.0 fixes the issue.

9.9 **CVE-2026-48750**

Incus is a system container and virtual machine manager. Prior to version 7.2.0, the `record-output` parameter of the `/instances/$name/exec` endpoint stores the output of the command in the `exec-output` directory of the instance. If `exec-output` is a symlin

9.9 **CVE-2026-48751**

Incus is a system container and virtual machine manager. Prior to version 7.2.0, instance snapshots ignore the `restricted.containers.lowlevel=block` setting; allowing for arbitrary command execution on the Incus server by abusing lowlevel hooks such as `raw.l

9.9 **CVE-2026-48752**

Incus is a system container and virtual machine manager. Prior to version 7.2.0, a specially crafted image or instance backup can be used to read or create/write arbitrary files on the host; possibly leading to arbitrary command execution. Version 7.2.0 patche

9.9 **CVE-2026-48753**

Incus is a system container and virtual machine manager. Prior to version 7.1.0, the S3 protocol upload endpoint is vulnerable to path traversal and allows creation of arbitrary files on the host. This behavior could lead to arbitrary command execution. Versio

9.9 **CVE-2026-48755**

Incus is a system container and virtual machine manager. Prior to version 7.1.0, improper validation of user-provided backup compression algorithm leads to argument injection in the constructed command line. This leads to an arbitrary file write on the host, p

9.9 **CVE-2026-48769**

Incus is a system container and virtual machine manager. Prior to version 7.2.0, an arbitrary file write exists in the Incus client when a malicious image server returns a crafted `Incus-Image-Hash` header. This can lead to arbitrary command execution as root

9.9 **CVE-2026-62867**

Incus is a system container and virtual machine manager. Prior to version 7.3.0, improper validation of user-provided `block.create_options` in storage volume configuration leads to argument injection in the constructed filesystem creation command line. This a

9.9 **CVE-2026-62940**

Incus is a system container and virtual machine manager. Prior to version 7.3.0, when migrating an instance to another cluster member, user-supplied configuration overrides (including security-critical keys like `security.privileged` and `raw.lxc`) are applied

9.9 **CVE-2026-62941**

Incus is a system container and virtual machine manager. Prior to version 7.3.0, when copying an instance across projects, the project restriction check (`AllowInstanceCreation`) runs BEFORE the source instance's configuration is merged into the request. Dange

9.9 **CVE-2026-63125**

Incus is a system container and virtual machine manager. Prior to version 7.3.0, an unprivileged, project-confined Incus user (a non-admin TLS/RBAC identity with `can_create_images` and `can_create_instances`) can execute arbitrary code as root on the host. A

9.9 **CVE-2026-63343**

Incus is a system container and virtual machine manager. Prior to version 7.3.0, a malicious image containing a `metadata.yaml` symlink pointing to an arbitrary host path allows an authenticated Incus user to read or overwrite any file on the host as root via

9.9 **CVE-2026-77810**

In the Neptune connector, a user with access to Neptune through Athena Federated Query could gain access to properties in the Lambda supplying the compute for the connector. To remediate this issue, users should upgrade to aws-athena-query-federation v2026.30.

9.9 **CVE-2026-62283**

Nezha Monitoring is a self-hostable, lightweight, servers and websites monitoring and O&M tool. Nezha versions 1.14.13 through 1.14.14 and 2.0.0 through 2.0.9 do not bind stream identifiers created by CreateStream in service/rpc/io_stream.go to their creating

9.8 **CVE-2026-77649**

The internment crate 0.8.7 for Rust can trigger execution of malicious code when compiling a project that uses the crate, because it has a rogue dependency that registers with a command-and-control server to offer arbitrary code execution.

9.8 **CVE-2026-77650**

The append-only-vec crate 0.1.9 for Rust can trigger execution of malicious code when compiling a project that uses the crate, because it has a rogue dependency that registers with a command-and-control server to offer arbitrary code execution.

9.8 **CVE-2026-77651**

The arrayref crate 0.3.10 for Rust can trigger execution of malicious code when compiling a project that uses the crate, because it has a rogue dependency that registers with a command-and-control server to offer arbitrary code execution.

20 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.