Daily brief, Friday, May 22, 2026

May 21, 8:00 PM to May 22, 8:00 PM ET

Generated Nov 6, 2026, 11:56 PM ET

0	1	0	25	0	0
Breaking	Newly exploited	Exploit code	Critical CVEs	Ransomware posts	New breaches

1 newly exploited, 25 new critical CVEs.

Breaking

Nothing spreading fast in technology large companies run.

Newly exploited in the wild

1

9.8 **CVE-2026-9082** Drupal Core CISA KEV DETECTION

SQL injection in Drupal Core's database abstraction API lets an attacker escalate privileges and execute remote code via crafted requests.

New public exploit code

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

New critical CVEs

25

9.8 **CVE-2026-9082** Drupal Core KEV EXPLOIT CODE DETECTION

SQL injection in Drupal Core's database abstraction API lets an attacker escalate privileges and execute remote code via crafted requests.

10.0 **CVE-2026-46595** Golang crypto

Previously, CVE-2024-45337 fixed an authorization bypass for misused ssh server configurations; if any other type of callback is passed other than public key, then the source-address validation would be skipped.

10.0 **CVE-2026-40412** Microsoft azure orbital spatio

Unrestricted upload of file with dangerous type in Azure Orbital Spatio allows an unauthorized attacker to execute code over a network.

10.0 **CVE-2026-42901** Microsoft entra id

Origin validation error in Microsoft Entra ID allows an unauthorized attacker to elevate privileges over a network.

10.0 **CVE-2026-47280** Microsoft azure resource manager

Improper authentication in Azure Resource Manager (ARM) allows an unauthorized attacker to elevate privileges over a network.

9.9 **CVE-2026-40411** Microsoft azure virtual network gateway

Improper input validation in Azure Virtual Network Gateway allows an authorized attacker to execute code over a network.

9.6 **CVE-2026-39821** Golang net

The ToASCII and ToUnicode functions incorrectly accept Punycode-encoded labels that decode to an ASCII-only label. For example, ToUnicode("xn--example-.com") incorrectly returns the name "example.com" rather than an error. This behavior can lead to privilege e

9.3 **CVE-2026-41090** Microsoft 365 copilot

Improper neutralization of special elements used in a command ('command injection') in Microsoft Copilot allows an unauthorized attacker to perform tampering over a network.

9.1 **CVE-2026-39830** Golang crypto

A malicious SSH peer could send unsolicited global request responses to fill an internal buffer, blocking the connection's read loop. The blocked goroutine could not be released by calling Close(), resulting in a resource leak per connection. Unsolicited globa

9.1 **CVE-2026-39831** Golang crypto

The Verify() method for FIDO/U2F security key types (sk-ecdsa-sha2-nistp256@openssh.com, sk-ssh-ed25519@openssh.com) did not check the User Presence flag. Signatures generated without physical touch were accepted, allowing unattended use of a hardware security

9.1 **CVE-2026-39832** Golang crypto

When adding a key to a remote agent constraint extensions such as restrict-destination-v00@openssh.com were not serialized in the request. Destination restrictions were silently stripped when forwarding keys, allowing unrestricted use of the key on the remote

9.1 **CVE-2026-39833** Golang crypto

The in-memory keyring returned by NewKeyring() silently accepted keys with the ConfirmBeforeUse constraint but never enforced it. The key would sign without any confirmation prompt, with no indication to the caller that the constraint was not in effect. NewKey

9.1 **CVE-2026-39834** Golang crypto

When writing data larger than 4GB in a single Write call on an SSH channel, an integer overflow in the internal payload size calculation caused the write loop to spin indefinitely, sending empty packets without making progress. The size comparison now uses int

9.1 **CVE-2026-42508** Golang crypto

Previously, a revoked 'SignatureKey' belonging to a CA was not correctly checked for revocation. Now, both the 'key' and 'key.SignatureKey' are checked for @revoked.

9.1 **CVE-2026-33843** Microsoft entra id

Authentication bypass using an alternate path or channel in Microsoft Azure Active Directory B2C allows an unauthorized attacker to elevate privileges over a network.

10.0 **CVE-2026-33712**

Typebot is a chatbot builder tool. In versions 3.15.2 and prior, the preview chat endpoint (POST /api/v1/typebots/{typebotId}/preview/startChat) allows unauthenticated users to achieve Server-Side Request Forgery (SSRF) by supplying a custom typebot definition

10.0 **CVE-2026-23652** Microsoft power pages

Improper neutralization of special elements used in a command ('command injection') in Microsoft Power Pages allows an unauthorized attacker to execute code over a network.

10.0 **CVE-2026-41104** Microsoft planetary computer

Deserialization of untrusted data in Microsoft Planetary Computer Pro allows an unauthorized attacker to disclose information over a network.

9.8 **CVE-2026-44930** Apache cxf

An LDAP injection vulnerability in the LDAP Certificate repository of the XKMS server in Apache CXF may allow an attacker to retrieve arbitrary certificates from the repository. Users are recommended to upgrade to versions 4.2.1, 4.1.6 or 3.6.11, which fix thi

9.8 **CVE-2026-32253** Lizardbyte sunshine

Sunshine is a self-hosted game stream host for Moonlight. In versions prior to 2026.516.143833, the client-certificate authentication can be bypassed because of how OpenSSL verification results are handled. In src/crypto.cpp, the custom verify callback treats

5 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. Leak-site data: RansomLook (ransomlook.io), CC BY 4.0; sectors grouped and countries mapped by Watch Floor. CVE IDs link to the full record on Watch Floor.