Daily brief, Thursday, July 2, 2026

Jul 1, 8:00 PM to Jul 2, 8:00 PM ET

Generated Nov 4, 2026, 5:28 AM ET

0	0	0	31	0	0
Breaking	Newly exploited	Exploit code	Critical CVEs	Ransomware posts	New breaches

31 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

31

9.9 **CVE-2026-45499** Microsoft azure openai

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

9.9 **CVE-2026-57100** Microsoft entra provisioning service

Server-side request forgery (ssrf) in Microsoft Entra Provisioning Service (SyncFabric) allows an authorized attacker to elevate privileges over a network.

9.3 **CVE-2026-41106** Microsoft 365 copilot

Url redirection to untrusted site ('open redirect') in M365 Copilot allows an unauthorized attacker to elevate privileges over a network.

10.0 **CVE-2026-57624**

Unauthenticated Remote Code Execution (RCE) in Blocksy Companion Pro <= 2.1.46 versions.

10.0 **CVE-2026-50746** Ui unifi connect application

A malicious actor with access to the network could exploit an Improper Access Control vulnerability found in UniFi Connect Application to execute a Command Injection on the host device.

10.0 **CVE-2026-56004**

A shellcode injection in the mercurial handler of the obs tar_scm source service before version 0.12.4 could be used by attackers able to provide a _service file to execute code as the source service or the local user checking out the malicious services

9.9 **CVE-2026-27419**

Subscriber Arbitrary File Upload in Zegen <= 1.1.9 versions.

9.9 **CVE-2026-50747** Ui unifi talk application

A malicious actor with access to the network and low privileges could exploit a series of authenticated SQL Injection vulnerabilities found in UniFi Talk Application to escalate privileges on the host device.

9.9 **CVE-2026-50748** Ui unifi access

+1 more CVEs in the same release

A malicious actor with access to the network and low privileges could exploit an Improper Input Validation vulnerability found in UniFi Access Application to execute a Command Injection on the host device.

9.9 **CVE-2026-55115** Ui unifi protect

A malicious actor with access to the network and low privileges could exploit a Server-Side Request Forgery (SSRF) in UniFi Protect Application to escalate privileges on the host device.

9.9 **CVE-2026-44935** Suse rancher fleet

Missing validation of "valuesFrom" references in Helm Deployer of SUSE Rancher Fleet 0.15 before 0.15.2, 0.14 before 0.14.6, 0.13 before 0.13.11 and 0.12 before 0.12.15 could be used by owners of one tenant to access fleet credentials of other tenants.

9.8 **CVE-2026-57621**

Unauthenticated PHP Object Injection in Booktics <= 1.0.21 versions.

9.8 **CVE-2026-57677**

Unauthenticated PHP Object Injection in Novalnet Payment Gateway for WooCommerce <= 12.10.3 versions.

9.8 **CVE-2026-5524** DETECTION

The Divi Form Builder plugin for WordPress is vulnerable to Arbitrary File Upload leading to Remote Code Execution in all versions up to and including 5.1.8. This is due to insufficient file extension validation in the do_image_upload() function where user-sup

9.8 **CVE-2026-4767**

Missing authentication for critical function vulnerability in TR7 Cyber ??Defense Inc. WAF-ASP allows Authentication Abuse. This issue affects WAF-ASP: from v1.0.324.900 before v1.4.0.117.

9.8 **CVE-2026-58455** DETECTION

Dockwatch through 0.6.567 contains an unauthenticated OS command injection vulnerability that allows remote attackers to execute arbitrary shell commands by exploiting a missing exit() after an authentication redirect in loader.php combined with unsanitized in

9.8 **CVE-2022-50973**

Yonyou KSOA 9.0 contains an unauthenticated arbitrary file upload vulnerability in the com.sksoft.bill.ImageUpload servlet that allows unauthenticated attackers to upload arbitrary files by submitting a POST request with attacker-controlled filepath and filena

9.8 **CVE-2024-14037**

Redsea Cloud eHR contains an arbitrary file upload vulnerability that allows unauthenticated attackers to achieve remote code execution by uploading malicious files through the PtFjk.mob servlet endpoint. Attackers can submit a multipart POST request with a JS

9.8 **CVE-2026-58466**

AutoBangumi before 3.2.8 contains a hard-coded default credentials vulnerability that allows unauthenticated attackers to authenticate as the administrator by using the publicly known default credentials seeded at startup via add_default_user() in the database

9.8 **CVE-2026-38968** Ntop ntopng

ntopng through 6.6 is vulnerable to Predictable Session Identifier which can lead to Session Hijacking. HTTP session identifiers in src/HTTPserver.cpp use weak time-seeded pseudo-randomness during session creation. As a result, fresh authenticated logins can r

10 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.