Daily brief, Monday, August 3, 2026

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

Generated Nov 2, 2026, 11:38 PM ET

0	1	0	52	0	0
Breaking	Newly exploited	Exploit code	Critical CVEs	Ransomware posts	New breaches

1 newly exploited, 52 new critical CVEs.

Breaking

Nothing spreading fast in technology large companies run.

Newly exploited in the wild

1

8.2 **CVE-2026-18577** N-able N-central CISA KEV DETECTION

An attacker can bypass authentication and take over accounts in N-able N-central.

New public exploit code

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

New critical CVEs

52

9.8 **CVE-2026-41452** Krayin laravel-crm EXPLOIT CODE DETECTION

Krayin CRM 2.2.4 contains a missing authentication vulnerability in the installer middleware that allows unauthenticated remote attackers to overwrite the primary administrator account by sending a crafted HTTP POST request with the X-Requested-With: XMLHttpRe

10.0 **CVE-2026-69084** Siyuan-Note siyuan EXPLOIT CODE DETECTION

SiYuan versions <= v3.7.2 expose the /api/search/searchEmbedBlock endpoint, which passes a client-supplied SQL statement verbatim to the main read-write siyuan.db handle with no single-statement, read-only, or admin restrictions. The endpoint is gated only by

10.0 **CVE-2026-69085** Siyuan-Note siyuan EXPLOIT CODE DETECTION

SiYuan before v3.7.3 contains a SQL injection vulnerability in the /api/filetree/searchDocs endpoint, where the caller-supplied keyword parameter is concatenated directly into SQL statements with no escaping or parameter binding. The endpoint is reachable by a

9.1 **CVE-2026-59650** Bouncycastle bc-java

In Bouncy Castle for Java before 1.85, MTI/A0 DH agreement exponentiates unvalidated peer value. This issue also affects Bouncy Castle for Java LTS before 2.73.12.

9.1 **CVE-2026-8763** Bouncycastle bc-java

In Bouncy Castle for Java before 1.85, Name Constraints bypass via trailing dot in rfc822Name and URI. This issue also affects Bouncy Castle for Java LTS before 2.73.12, and Bouncy Castle for Java FIPS (BC-FJA) before bc-fips 1.0.2.7 (1.0.X series), 2.0.2 (2.0

9.1 **CVE-2026-58062** Bouncycastle bc-java

In Bouncy Castle for Java before 1.85, Stapled OCSP response accepted without binding to the checked certificate. This issue also affects Bouncy Castle for Java LTS before 2.73.12, and Bouncy Castle for Java FIPS (BC-FJA) before bc-fips 2.0.2 (2.0.X series) an

9.1 **CVE-2026-18248** Fastify fastify\/aws-lambda

@fastify/aws-lambda version 6.4.0 decorates each Fastify request with request.awsLambda.event and request.awsLambda.context, values that applications are documented to use for authorization decisions such as reading API Gateway authorizer claims. In the defaul

9.8 **CVE-2026-18612** GL-iNet GL-MT3000

A flaw has been found in GL-iNet GL-MT3000 up to 4.4.5. This vulnerability affects the function plugins.remove_package/plugins.install_package of the file /cgi-bin/glc of the component plugins.so Native Plugin. This manipulation causes command injection. The a

9.8 **CVE-2026-18601** GL.iNet GL-MT3000

A vulnerability was found in GL.iNet GL-MT3000 up to 4.4.5. This impacts the function ovpn-client.check_config of the file /cgi-bin/glc of the component ovpn-client.so Native Plugin. Performing a manipulation of the argument filename results in command injecti

9.8 **CVE-2026-18602** GL.iNet GL-MT3000

A vulnerability was determined in GL.iNet GL-MT3000 up to 4.4.5. Affected is the function ovpn-client.get_recommend_config of the file /cgi-bin/glc of the component ovpn-client.so Native Plugin. Executing a manipulation of the argument Hostname can lead to com

9.8 **CVE-2026-18613** GL-iNet GL-MT3000

A vulnerability has been found in GL-iNet GL-MT3000 up to 4.4.5. This issue affects the function plugins.set_config of the file /cgi-bin/glc of the component plugins.so Native Plugin. Such manipulation leads to injection. The attack can be launched remotely. T

9.8 **CVE-2026-64827** Telenia Software TVox

Telenia Software TVox 26.5.3 and prior 26.x versions, and 24.9.21 and prior 24.x versions, contain an authentication bypass vulnerability in set_env.php where the redirectToLoginAdminIRequestHaveAccessToken() function derives the current page name from PHP_SEL

9.1 **CVE-2026-9390** Xml\ \

XML::Sig versions before 0.71 for Perl allow XPath injection in ID lookup. verify() and _get_signed_xml() in lib/XML/Sig.pm build XPath expressions by concatenating the SignedInfo/Reference/@URI value read from the document being verified. The value is neither

10.0 **CVE-2026-69083** Siyuan-Note siyuan

SiYuan versions before v3.7.3 contain SQL injection vulnerabilities in the fullTextSearchAssetContent endpoint reachable by unauthenticated users and publish RoleReader tokens. Attackers can execute arbitrary SQL on the read-write asset-content database via un

9.8 **CVE-2026-18108** Timlegge net\

Net::SAML2 versions before 0.86 for Perl allow authentication bypass because _verify_encrypted_assertion accepts an EncryptedAssertion whose decrypted content carries no signature. _verify_encrypted_assertion decrypts the EncryptedAssertion and returns it as v

9.1 **CVE-2026-9487** Xml\ \

XML::Sig versions before 0.71 for Perl allow signature wrapping via duplicate ID. _get_signed_xml() in lib/XML/Sig.pm, called from verify(), resolves the SignedInfo Reference/@URI to a node with the XPath expression "//*[@ID='$id']" and returns the first node

10.0 **CVE-2026-33591**

A vulnerability in Wapt Server before version 2.6.1.17813 allows a remote unauthenticated attacker to bypass security restriction using a specially crafted packet and retrieve a valid session token for the targeted account.

10.0 **CVE-2026-48323** Adobe campaign

Adobe Campaign Classic (ACC) is affected by an Improper Neutralization of Special Elements Used in a Template Engine vulnerability that could result in arbitrary code execution in the context of the current user. An attacker could exploit this vulnerability to

10.0 **CVE-2026-48330** Adobe campaign

+1 more CVEs in the same release

Adobe Campaign Classic (ACC) is affected by an Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability that could result in arbitrary code execution in the context of the current user. An attacker could exploit this v

10.0 **CVE-2026-48331** Adobe campaign

Adobe Campaign Classic (ACC) is affected by a Server-Side Request Forgery (SSRF) vulnerability that could result in privilege escalation. Exploitation of this issue does not require user interaction. Scope is changed.

31 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.