Daily brief, Tuesday, May 12, 2026

May 11, 8:00 PM to May 12, 8:00 PM ET

Generated Nov 7, 2026, 1:56 AM ET

0	0	0	71	0	1
Breaking	Newly exploited	Exploit code	Critical CVEs	Ransomware posts	New breaches

71 new critical CVEs, 1 new breaches.

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

71

9.4 **CVE-2026-44262** Dedoc scramble EXPLOIT CODE DETECTION

Scramble generates API documentation for Laravel project. From 0.13.2 to before 0.13.22, when documentation endpoints are publicly accessible and validation rules reference user-controlled input, request supplied data may be evaluated during documentation gene

9.6 **CVE-2026-8043** Ivanti Xtraction

Ivanti Xtraction server. An attacker gains read access to sensitive files and ability to write arbitrary HTML files. Update Ivanti Xtraction to version 2026.2 or later to remediate this vulnerability.

9.9 **CVE-2026-42823** Microsoft azure logic apps

Improper access control in Azure Logic Apps allows an authorized attacker to elevate privileges over a network.

9.8 **CVE-2026-8401** Mozilla firefox

Sandbox escape in the Profile Backup component. This vulnerability was fixed in Firefox 150.0.3, Firefox ESR 115.36, Firefox ESR 140.11, and Thunderbird 140.11.

9.8 **CVE-2026-41293** Apache tomcat

Improper Input Validation vulnerability in Apache Tomcat. This issue affects Apache Tomcat: from 11.0.0-M1 through 11.0.21, from 10.1.0-M1 through 10.1.54, from 9.0.0.M1 through 9.0.117, from 10.0.0-M1 through 10.0.27. Older, end of support versions may also b

9.8 **CVE-2026-43512** Apache tomcat

DEPRECATED: Authentication Bypass Issues vulnerability in digest authentication in Apache Tomcat. This issue affects Apache Tomcat: from 11.0.0-M1 through 11.0.21, from 10.1.0-M1 through 10.1.54, from 9.0.0.M1 through 9.0.117, from 8.5.0 through 8.5.100, from

9.8 **CVE-2026-26083** Fortinet fortisandbox

A missing authorization vulnerability in Fortinet FortiSandbox 5.0.0 through 5.0.1, FortiSandbox 4.4.0 through 4.4.8, FortiSandbox 4.2 all versions, FortiSandbox Cloud 5.0.0 through 5.0.1, FortiSandbox Cloud 4.4.5 through 4.4.8, FortiSandbox PaaS 23.4 all vers

9.8 **CVE-2026-41089** Microsoft windows server 2012 DETECTION

Stack-based buffer overflow in Windows Netlogon allows an unauthorized attacker to execute code over a network.

9.8 **CVE-2026-41096** Microsoft windows 11 23h2

Heap-based buffer overflow in Microsoft Windows DNS allows an unauthorized attacker to execute code over a network.

9.8 **CVE-2026-44277** Fortinet fortiauthenticator

A improper access control vulnerability in Fortinet FortiAuthenticator 8.0.2, FortiAuthenticator 8.0.0, FortiAuthenticator 6.6.0 through 6.6.8, FortiAuthenticator 6.5.0 through 6.5.6, FortiAuthenticator 6.4.0 through 6.4.10 may allow attacker to execute unauth

9.3 **CVE-2026-40379** Microsoft entra id

Exposure of sensitive information to an unauthorized actor in Azure Entra ID allows an unauthorized attacker to perform spoofing over a network.

9.3 **CVE-2026-40402** Microsoft windows 11 23h2

Use after free in Windows Hyper-V allows an unauthorized attacker to elevate privileges locally.

9.1 **CVE-2026-43515** Apache tomcat

Improper Authorization vulnerability when multiple method constraints define an HTTP method for the same extension in Apache Tomcat. This issue affects Apache Tomcat: from 11.0.0-M1 through 11.0.21, from 10.1.0-M1 through 10.1.54, from 9.0.0.M1 through 9.0.117

9.1 **CVE-2026-33117** Microsoft azure sdk for java

The Java Key Vault Keys library in the Azure SDK for Java contains an issue in the local cryptographic verification path where authentication tag comparison was implemented incorrectly. In affected applications that use the vulnerable local cryptography path,

9.1 **CVE-2026-41103** Microsoft confluence saml sso

Incorrect implementation of authentication algorithm in Microsoft SSO Plugin for Jira & Confluence allows an unauthorized attacker to elevate privileges over a network.

9.8 **CVE-2026-42854** Espressif arduino-esp32

arduino-esp32 is an Arduino core for the ESP32, ESP32-S2, ESP32-S3, ESP32-C3, ESP32-C6 and ESP32-H2 microcontrollers. Prior to 3.3.8, the WebServer multipart form parser in arduino-esp32 allocates a Variable Length Array (VLA) on the stack whose size is derive

9.9 **CVE-2026-42196** Codingjoe django-s3file

django-s3file is a lightweight file upload input for Django and Amazon S3. Prior to 7.0.2, S3FileMiddleware is vulnerable to relative path traversal attacks, where an attacker can use a modified request to escape pre-signed upload locations and have the Django

9.3 **CVE-2026-44257** efwGrp efw4.X

efw4.X is an Enterprise Framework for Web. Prior to 4.08.010, efw.file.FileManager.unZip writes zip entries to disk using new File(baseDir, zipEntry.getName()) with no canonical-path check. An entry name such as ../../../pwned.jsp escapes the intended extracti

9.3 **CVE-2026-44258** efwGrp efw4.X

efw4.X is an Enterprise Framework for Web. Prior to 4.08.010, the elfinder_checkRisk function validates target and targets for path traversal and home containment, but does not validate the dst (destination) parameter used by elfinder_paste. An attacker can co

10.0 **CVE-2026-42288**

ChurchCRM is an open-source church management system. Prior to 7.3.2, The fix for CVE-2026-39337 is incomplete. The pre-authentication remote code execution vulnerability in ChurchCRM's setup wizard via unsanitized DB_PASSWORD remains fully exploitable This vu

51 more critical CVEs in this window: see the dashboard

Ransomware

No leak-site posts collected.

New data breaches 1

Cushman & Wakefield cushmanwakefield.com 310,431 accounts

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.