Daily brief, Tuesday, July 28, 2026

Jul 27, 8:00 PM to Jul 28, 8:00 PM ET

Generated Nov 3, 2026, 5:46 AM ET

0	0	0	18	0	1
Breaking	Newly exploited	Exploit code	Critical CVEs	Ransomware posts	New breaches

18 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

18

9.8 **CVE-2026-66713** Apache axis2Vjava

Deserialization of Untrusted Data (CWE-502) in the Tribes-based clustering component in Apache Software Foundation Apache Axis2/Java through 2.0.0 on Apache Tomcat (only when Tribes clustering is enabled, which is off by default) allows an unauthenticated remo

10.0 **CVE-2026-11756**

A Deserialization of Untrusted Data vulnerability affecting Station Launcher App in 3DEXPERIENCE platform from Release 3DEXPERIENCE R2023x through Release 3DEXPERIENCE R2026x could lead to an unauthenticated remote code execution.

10.0 **CVE-2026-65880**

Joomla Extension - balbooa.com - Unauthenticated remote code execution in Balbooa Forms < 2.4.3 - An insecure form processing logic allowed code execution for forms that include the signature field type.

10.0 **CVE-2026-16498**

The terraform-mcp-server before version 1.1.0 is vulnerable to a cross-tenant credential reuse issue in the streamable-HTTP stateless transport mode that may allow one user's Terraform token to be used to execute tool calls on behalf of subsequent users. This

9.8 **CVE-2026-14545**

The TrueBooker WordPress plugin before 1.2.4 does not validate account ownership when resetting a user's password through one of its front-end account handlers, allowing unauthenticated attackers to set an arbitrary password on any account, including an admini

9.8 **CVE-2026-15014**

The SMS Alert – SMS & OTP for WooCommerce, Order Notifications & Abandoned Cart Recovery plugin for WordPress is vulnerable to Authentication Bypass leading to Account Takeover in all versions up to, and including, 3.9.7 via the `billing_phone` parameter. This

9.8 **CVE-2026-16462**

In PROCON-WEB SCADA the endpoint 'GetGridData' is not properly sanitized. This allows a remote unauthenticated attacker to execute arbitrary SQL commands.

9.8 **CVE-2026-14446** Ibm websphere application server

IBM WebSphere Application Server 9.0, and 8.5 is vulnerable to broken access control/privilege escalation in the administrative console.

9.8 **CVE-2026-14512** Ibm websphere application server

IBM WebSphere Application Server 9.0, and 8.5 traditional is vulnerable to pre-authentication unsafe deserialization which could allow a remote attacker to bypass authentication or execute arbitrary code.

9.8 **CVE-2026-54658**

Hypequery is a TypeScript semantic layer for ClickHouse. Prior to 2.5.1, escapeValue() in packages/clickhouse/src/core/utils.ts did not escape backslashes before single quotes during parameter substitution, allowing attacker controlled query parameters with a

9.4 **CVE-2026-11841**

An attacker may perform unauthenticated read and write operations on sensitive filesystem areas via the AppEngine Fileaccess over HTTP due to improper access restrictions. A critical filesystem directory was unintentionally exposed through the HTTP-based file

9.4 **CVE-2026-6881**

A SQL Injection in the Giving Reports functionality in Ellucian Advance Web and Legacy Advance allows an authenticated attacker to extract sensitive information from databases via a crafted SQL query in the class credit field. This issue affects Advance Web: a

9.3 **CVE-2026-14973** Ibm aspera

IBM Aspera Desktop App 1.0.5 through 1.0.19 IBM Aspera for desktop can allow files to be written outside of the user's selected download destination.

9.2 **CVE-2026-67174**

Pivotick contains a DOM-based cross-site scripting vulnerability in its generic UI element resolution and icon-rendering utilities. The tryResolveHTMLElement function treated any resolved string as HTML markup by assigning it to a <template> element through in

9.1 **CVE-2026-14958** Ibm aspera faspex

+1 more CVEs in the same release

IBM Aspera Faspex 5 5.0.0 through 5.0.15.4 could allow a remote authenticated attacker to execute arbitrary code due to unquoted shell interpolation.

9.1 **CVE-2026-62325**

goshs is a feature-rich single-binary file server for red teamers and developers. From 2.1.3 until 2.1.4, the sftpserver/sftpserver.go password handler used Username != "" && Password != "", so running goshs with -b 'admin:' -sftp and no -fkf left both SFTP au

9.1 **CVE-2026-64863**

goshs is a feature-rich single-binary file server for red teamers and developers. Prior to 2.1.4, the httpserver/server.go wdGuard handled WebDAV MOVE as a write-only method and did not enforce --no-delete, allowing WebDAV clients to delete or overwrite files

Ransomware

No leak-site posts collected.

New data breaches 1

Houston City College hccs.edu 831,642 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. CVE IDs link to the full record on Watch Floor.