Daily brief, Tuesday, August 18, 2026

Aug 17, 8:00 PM to Aug 18, 8:00 PM ET

Generated Nov 2, 2026, 9:18 AM ET

0	4	0	226	0	0
Breaking	Newly exploited	Exploit code	Critical CVEs	Ransomware posts	New breaches

4 newly exploited, 226 new critical CVEs.

Breaking

Nothing spreading fast in technology large companies run.

Newly exploited in the wild

4

9.8 **CVE-2026-65400** Apple macOS CISA KEV

An attacker gains unauthorized access to Screen Sharing on Apple macOS without authentication.

9.8 **CVE-2026-59310** Broadcom VMware vCenter CISA KEV

An attacker gains remote code execution and unauthorized access to sensitive data on Broadcom VMware vCenter without authentication.

9.8 **CVE-2026-33824** Microsoft Internet Key Exchange (IKE) Service Extensions CISA KEV DETECTION

An attacker gains remote code execution on Microsoft Internet Key Exchange (IKE) Service Extensions without authentication.

9.1 **CVE-2026-55040** Microsoft SharePoint CISA KEV DETECTION

An attacker gains unauthorized access to sensitive information and potentially executes arbitrary code on Microsoft SharePoint.

New public exploit code

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

New critical CVEs

226

9.1 **CVE-2026-55040** Microsoft SharePoint KEV EXPLOIT CODE DETECTION

An attacker gains unauthorized access to sensitive information and potentially executes arbitrary code on Microsoft SharePoint.

9.8 **CVE-2026-59310** Broadcom VMware vCenter KEV EXPLOIT CODE

An attacker gains remote code execution and unauthorized access to sensitive data on Broadcom VMware vCenter without authentication.

9.8 **CVE-2026-65400** Apple macOS KEV EXPLOIT CODE

An attacker gains unauthorized access to Screen Sharing on Apple macOS without authentication.

9.8 **CVE-2026-33824** Microsoft Internet Key Exchange (IKE) Service Ex… KEV EXPLOIT CODE DETECTION

An attacker gains remote code execution on Microsoft Internet Key Exchange (IKE) Service Extensions without authentication.

9.1 **CVE-2026-18963** Red Hat Red Hat build of Keycloak 26.4 EXPLOIT CODE DETECTION

Affected: Red Hat Build of Keycloak, specifically the keycloak-services component. Attacker gains: Ability to force password reset for any user without authentication. Recommended action: Immediately update to the latest version of Red Hat Build of Keycloak th

9.8 **CVE-2026-74987** Mozilla firefox

Internally found bugs present in Firefox ESR 140.13, Firefox ESR 153.0 and Firefox 153. Some of these bugs showed evidence of memory corruption or another security-relevant defect and we presume that with enough effort some of these could have been exploited.

9.8 **CVE-2026-74990** Mozilla firefox

Internally found bugs present in Firefox ESR 115.38, Firefox ESR 140.13, Firefox ESR 153.0 and Firefox 153. Some of these bugs showed evidence of memory corruption or another security-relevant defect and we presume that with enough effort some of these could h

9.8 **CVE-2026-74988** Mozilla firefox

Internally found bugs present in Firefox ESR 153.0 and Firefox 153. Some of these bugs showed evidence of memory corruption or another security-relevant defect and we presume that with enough effort some of these could have been exploited. This vulnerability w

9.8 **CVE-2026-74989** Mozilla firefox

Internally found bugs present in Firefox 153. Some of these bugs showed evidence of memory corruption or another security-relevant defect and we presume that with enough effort some of these could have been exploited. This vulnerability was fixed in Firefox 15

10.0 **CVE-2026-75874** Mozilla firefox

Sandbox escape in the Remote Settings Client component. This vulnerability was fixed in Firefox 154, Thunderbird 154, Firefox ESR 115.40, Firefox ESR 140.15, Firefox ESR 153.2, Thunderbird 140.15, and Thunderbird 153.2.

10.0 **CVE-2026-61241** Oracle internet directory

+2 more CVEs in the same release

Vulnerability in the Oracle Internet Directory product of Oracle Fusion Middleware (component: OID LDAP Server). Supported versions that are affected are 12.2.1.4.0 and 14.1.2.1.0. Easily exploitable vulnerability allows unauthenticated attacker with network a

10.0 **CVE-2026-70880** Oracle hyperion data relationship management

+6 more CVEs in the same release

Vulnerability in the Oracle Hyperion Data Relationship Management product of Oracle Hyperion (component: Access and security). The supported version that is affected is 11.2.25.0.000. Easily exploitable vulnerability allows unauthenticated attacker with networ

10.0 **CVE-2026-70921** Oracle hyperion financial management

+3 more CVEs in the same release

Vulnerability in the Oracle Hyperion Financial Management product of Oracle Hyperion (component: Security). The supported version that is affected is 11.2.25.0.000. Easily exploitable vulnerability allows unauthenticated attacker with network access via TLS to

9.9 **CVE-2026-60702** Oracle weblogic server

+3 more CVEs in the same release

Vulnerability in the Oracle WebLogic Server product of Oracle Fusion Middleware (component: Core). Supported versions that are affected are 12.2.1.4.0, 14.1.1.0.0, 14.1.2.0.0 and 15.1.1.0.0. Easily exploitable vulnerability allows low privileged attacker with

9.9 **CVE-2026-60720** Oracle identity manager

+3 more CVEs in the same release

Vulnerability in the Oracle Identity Manager product of Oracle Fusion Middleware (component: OIM Legacy UI). Supported versions that are affected are 12.2.1.4.0 and 14.1.2.1.0. Easily exploitable vulnerability allows low privileged attacker with network access

9.9 **CVE-2026-60730** Oracle webcenter portal

Vulnerability in the Oracle WebCenter Portal product of Oracle Fusion Middleware (component: Composer). Supported versions that are affected are 12.2.1.4.0 and 14.1.2.0.0. Easily exploitable vulnerability allows low privileged attacker with network access via

9.9 **CVE-2026-60916** Oracle webcenter enterprise capture

+6 more CVEs in the same release

Vulnerability in the Oracle WebCenter Enterprise Capture product of Oracle Fusion Middleware (component: Client Bundle). Supported versions that are affected are 12.2.1.4.0 and 14.1.2.0.0. Easily exploitable vulnerability allows unauthenticated attacker with n

9.9 **CVE-2026-60990** Oracle identity manager connector

+1 more CVEs in the same release

Vulnerability in the Oracle Identity Manager Connector product of Oracle Fusion Middleware (component: Core). Supported versions that are affected are 12.2.1.4.0 and 14.1.2.1.0. Easily exploitable vulnerability allows low privileged attacker with network acces

9.9 **CVE-2026-61003** Oracle managed file transfer

Vulnerability in the Oracle Managed File Transfer product of Oracle Fusion Middleware (component: MFT Runtime Server). Supported versions that are affected are 12.2.1.4.0 and 14.1.2.0.0. Easily exploitable vulnerability allows low privileged attacker with netw

9.9 **CVE-2026-61021** Oracle webcenter sites

+4 more CVEs in the same release

Vulnerability in the Oracle WebCenter Sites product of Oracle Fusion Middleware (component: WebCenter Sites). Supported versions that are affected are 12.2.1.4.0 and 14.1.2.0.0. Easily exploitable vulnerability allows low privileged attacker with network acces

178 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.