Daily brief, Tuesday, July 21, 2026

Jul 20, 8:00 PM to Jul 21, 8:00 PM ET

Generated Nov 3, 2026, 11:55 AM ET

0	4	0	300	0	0
Breaking	Newly exploited	Exploit code	Critical CVEs	Ransomware posts	New breaches

4 newly exploited, 300 new critical CVEs.

Breaking

Nothing spreading fast in technology large companies run.

Newly exploited in the wild

4

9.8 **CVE-2026-0770** Langflow Langflow CISA KEV

An attacker gains remote code execution on Langflow without authentication.

9.8 **CVE-2026-63030** WordPress Core CISA KEV

An attacker gains remote code execution on WordPress Core with user interaction.

8.1 **CVE-2021-27137** DD-WRT DD-WRT CISA KEV

An attacker can execute arbitrary code on a DD-WRT server without authentication by overflowing an internal buffer.

5.9 **CVE-2026-60137** WordPress Core CISA KEV

An attacker gets remote code execution on default WordPress installations without authentication or user interaction.

New public exploit code

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

New critical CVEs

300

9.8 **CVE-2026-63030** WordPress Core KEV EXPLOIT CODE

An attacker gains remote code execution on WordPress Core with user interaction.

9.8 **CVE-2026-0770** Langflow Langflow KEV EXPLOIT CODE

An attacker gains remote code execution on Langflow without authentication.

10.0 **CVE-2026-60264** Oracle coherence

+61 more CVEs in the same release

Vulnerability in the Oracle Coherence product of Oracle Fusion Middleware (component: Core). Supported versions that are affected are 14.1.1.0.0, 14.1.2.0.0 and 15.1.1.0.0. Easily exploitable vulnerability allows unauthenticated attacker with network access vi

10.0 **CVE-2026-61065** Oracle access manager

+5 more CVEs in the same release

Vulnerability in the Oracle Access Manager product of Oracle Fusion Middleware (component: Authentication Engine). 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

10.0 **CVE-2026-60663** Oracle webcenter content

+2 more CVEs in the same release

Vulnerability in the Oracle WebCenter Content product of Oracle Fusion Middleware (component: Web Content Management). 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-2026-61041** Oracle demantra demand management

Vulnerability in the Oracle Demantra Demand Management product of Oracle Supply Chain (component: Product Security). Supported versions that are affected are 12.2.3-12.2.15. Easily exploitable vulnerability allows low privileged attacker with network access vi

9.9 **CVE-2026-61072** Oracle peoplesoft enterprise fin staffing front office brazil

Vulnerability in the PeopleSoft Enterprise FIN Staffing Front Office Brazil product of Oracle PeopleSoft (component: Staffing). The supported version that is affected is 9.1. Easily exploitable vulnerability allows low privileged attacker with network access v

9.9 **CVE-2026-61076** Oracle peoplesoft enterprise hcm talent acquisition manager

Vulnerability in the PeopleSoft Enterprise HCM Talent Acquisition Manager product of Oracle PeopleSoft (component: Job Opening). The supported version that is affected is 9.2. Easily exploitable vulnerability allows low privileged attacker with network access

9.1 **CVE-2026-61059** Oracle peoplesoft enterprise scm order management

Vulnerability in the PeopleSoft Enterprise SCM Order Management product of Oracle PeopleSoft (component: Security). The supported version that is affected is 9.2. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to

10.0 **CVE-2026-16367** Mozilla firefox

Sandbox escape due to invalid pointer in the Disability Access APIs component. This vulnerability was fixed in Firefox 153 and Thunderbird 153.

10.0 **CVE-2026-47056** Oracle data integrator

Vulnerability in the Oracle Data Integrator product of Oracle Fusion Middleware (component: Rest Service). Supported versions that are affected are 12.2.1.4.0 and 14.1.2.0.0. Easily exploitable vulnerability allows unauthenticated attacker with network access

10.0 **CVE-2026-60360** Oracle unified directory

+3 more CVEs in the same release

Vulnerability in the Oracle Unified Directory product of Oracle Fusion Middleware (component: OUD Core). 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 access vi

10.0 **CVE-2026-60365** Oracle http server

+1 more CVEs in the same release

Vulnerability in the Oracle Weblogic Server Proxy Plug-in product of Oracle Fusion Middleware (component: WebLogic Server Proxy Plug-In for Third-Party Web Servers). The supported version that is affected is 15.1.1.0.0. Easily exploitable vulnerability allows

10.0 **CVE-2026-60379** Oracle service delivery platform

+15 more CVEs in the same release

Vulnerability in the Service Delivery Platform product of Oracle Fusion Middleware (component: Messaging Enabler). Supported versions that are affected are 12.2.1.4.0 and 14.1.2.0.0. Easily exploitable vulnerability allows unauthenticated attacker with network

9.9 **CVE-2026-60206** Oracle weblogic server

+10 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-2026-60402** Oracle timesten in-memory database

Vulnerability in the TimesTen In-Memory Database product of Oracle TimesTen In-Memory Database (component: Kubernetes Operator). The supported version that is affected is 26.1.1.1.0. Easily exploitable vulnerability allows low privileged attacker with network

9.9 **CVE-2026-60422** Oracle unified directory

Vulnerability in the Oracle Unified Directory product of Oracle Fusion Middleware (component: OUD Core). The supported version that is affected is 14.1.2.1.0. Easily exploitable vulnerability allows low privileged attacker with network access via LDAP to compr

9.9 **CVE-2026-60445** Oracle webcenter enterprise capture

+10 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 low privileged attacker with ne

9.9 **CVE-2026-60531** Oracle identity manager connector

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-2026-60537** Oracle managed file transfer

+1 more CVEs in the same release

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

172 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.