Daily brief, Tuesday, July 14, 2026

Jul 13, 8:00 PM to Jul 14, 8:00 PM ET

Generated Nov 3, 2026, 6:27 PM ET

0	4	0	78	0	0
Breaking	Newly exploited	Exploit code	Critical CVEs	Ransomware posts	New breaches

4 newly exploited, 78 new critical CVEs.

Breaking

Nothing spreading fast in technology large companies run.

Newly exploited in the wild

4

10.0 **CVE-2026-15409** SonicWall SMA1000 Appliances CISA KEV DETECTION

An attacker gains remote code execution and full system compromise on SonicWall SMA1000 Appliances.

7.8 **CVE-2026-56155** Microsoft Active Directory Federation Services CISA KEV

An authorized attacker elevates privileges locally in Microsoft's Active Directory Federation Services due to insufficient access control.

7.2 **CVE-2026-15410** SonicWall SMA1000 Appliances CISA KEV DETECTION

An attacker gains remote code execution on SonicWall SMA1000 Appliances.

5.3 **CVE-2026-56164** Microsoft SharePoint Server CISA KEV

An attacker gains ability to perform arbitrary file operations on Microsoft SharePoint Server.

New public exploit code

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

New critical CVEs

78

10.0 **CVE-2026-15409** SonicWall SMA1000 Appliances KEV EXPLOIT CODE DETECTION

An attacker gains remote code execution and full system compromise on SonicWall SMA1000 Appliances.

9.3 **CVE-2026-48356** Adobe Adobe Commerce KEV EXPLOIT CODE

Adobe Commerce is affected by an Unrestricted Upload of File with Dangerous Type vulnerability that could result in arbitrary code execution in the context of the current user, potentially gaining elevated access or control over the victim's account or session

9.1 **CVE-2026-59084** Apache tomcat

Insufficient Technical Documentation vulnerability in Apache Tomcat since the requirements to securely configure the EncryptInterceptor were not clearly documented. This issue affects Apache Tomcat: from 11.0.0-M1 through 11.0.23, from 10.1.0-M1 through 10.1.5

9.9 **CVE-2026-57092** Microsoft windows 10 1607

Use after free in Windows VMSwitch allows an authorized attacker to elevate privileges over a network.

9.8 **CVE-2026-42990** Microsoft windows 10 1607

Heap-based buffer overflow in SQL Server ODBC driver allows an unauthorized attacker to execute code over a network.

9.8 **CVE-2026-49172** Microsoft windows 10 1607

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

9.8 **CVE-2026-54117** Microsoft sql server 2016

+1 more CVEs in the same release

Deserialization of untrusted data in SQL Server allows an unauthorized attacker to execute code over a network.

9.8 **CVE-2026-54990** Microsoft windows 11 24h2

Heap-based buffer overflow in Remote Desktop Client allows an unauthorized attacker to execute code over a network.

9.8 **CVE-2026-50447** Microsoft windows 10 1607

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

9.8 **CVE-2026-50518** Microsoft windows 10 1607

+1 more CVEs in the same release

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

9.8 **CVE-2026-56188** Microsoft windows 10 1607

Concurrent execution using shared resource with improper synchronization ('race condition') in Windows Server Network driver allows an unauthorized attacker to execute code over a network.

9.8 **CVE-2026-56190** Microsoft windows 10 1607

Use of uninitialized resource in Windows RDP allows an unauthorized attacker to execute code over a network.

9.6 **CVE-2026-48561** Microsoft 365 copilot

Improper neutralization of special elements used in a command ('command injection') in Copilot Chat (Microsoft Edge) allows an unauthorized attacker to execute code over a network.

9.6 **CVE-2026-55008** Microsoft exchange server

Improper neutralization of input during web page generation ('cross-site scripting') in Microsoft Exchange Server allows an unauthorized attacker to perform spoofing over a network.

9.6 **CVE-2026-50380** Microsoft windows 10 1607

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

9.6 **CVE-2026-15773** Google chrome

Use after free in Core in Google Chrome on Windows prior to 150.0.7871.125 allowed a remote attacker to potentially perform a sandbox escape via a crafted HTML page. (Chromium security severity: High)

9.3 **CVE-2026-49798** Microsoft windows 10 1607

Use after free in Windows Kernel allows an unauthorized attacker to elevate privileges locally.

9.1 **CVE-2026-27690** Sap approuter

Due to an HTTP Request Smuggling vulnerability in SAP Approuter, an unauthenticated attacker could send a specially crafted HTTP request that leads to request-response desynchronization. This could result in the exposure of user responses and cause the system

9.1 **CVE-2026-59083** Apache tomcat

Improper Handling of URL Encoding (Hex Encoding) vulnerability in Apache Tomcat's rewrite valve allowed security constraint bypass for some configurations. This issue affects Apache Tomcat: from 11.0.0-M1 through 11.0.23, from 10.1.0-M1 through 10.1.56, from 9

9.1 **CVE-2026-54058** Python pillow

Pillow is a Python imaging library. Prior to 12.3.0, when Pillow loads an uncompressed McIdas AREA image from a filename through the mmap raw codec path, attacker-controlled header words can set a row stride smaller than the natural row width, causing pixel ac

56 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.