Daily brief, Monday, August 24, 2026

Aug 23, 8:00 PM to Aug 24, 8:00 PM ET

Generated Nov 2, 2026, 3:50 AM ET

0	1	0	46	0	0
Breaking	Newly exploited	Exploit code	Critical CVEs	Ransomware posts	New breaches

1 newly exploited, 46 new critical CVEs.

Breaking

Nothing spreading fast in technology large companies run.

Newly exploited in the wild

1

10.0 **CVE-2026-21962** Oracle HTTP Server and Oracle Weblogic Server Proxy Plu… CISA KEV DETECTION

An attacker gains remote code execution on Oracle HTTP Server and Oracle Weblogic Server Proxy Plug-in.

New public exploit code

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

New critical CVEs

46

10.0 **CVE-2026-21962** Oracle HTTP Server and Oracle Weblogic Server… KEV EXPLOIT CODE DETECTION

An attacker gains remote code execution on Oracle HTTP Server and Oracle Weblogic Server Proxy Plug-in.

10.0 **CVE-2026-78167**

A weakness has been identified in EFM ipTIME T16000M 14.20.2. The impacted element is the function httpcon_check_session_url of the component Session Validation Handler. This manipulation causes improper authentication. Remote exploitation of the attack is pos

10.0 **CVE-2026-77995**

Joomla Extension - miniorange.com - Arbitrary account takeover in miniOrange OAuth Client < 3.2.0, OAuth Single Sign-On – OIDC SSO < 1.2.2, Login with Keycloak OAuth Single Sign-On (SSO) < 1.2.2, Single Sign-On for Educational Institutes < 1.2.2 - The manipula

9.9 **CVE-2026-78169**

A vulnerability was detected in UTT HiPER 1250GW up to 3.2.7-210907-180535. This impacts the function strcpy of the file /goform/aspRemoteApConfTempSend of the component HTTP Request Handler. Performing a manipulation of the argument Profile results in stack-b

9.9 **CVE-2026-66897** Canonical lxd

A path traversal vulnerability in LXD's instance template processing allows an attacker with container edit permissions, or any user launching a crafted image, to overwrite arbitrary files on the host system as root. When processing target template paths speci

9.9 **CVE-2026-32559**

Subscriber Arbitrary File Upload in UltimateAI <= 3.1.0 versions.

9.8 **CVE-2026-78168**

A security vulnerability has been detected in EFM ipTIME T24000M up to 14.20.0. This affects the function httpcon_check_session_url of the component Session Validation Handler. Such manipulation leads to improper authentication. The attack can be executed remo

9.8 **CVE-2026-78211**

4MOSAn GCB Doctor developed by 4MOSAn Security Technology has a OS Command Injection vulnerability. Unauthenticated remote attackers can inject malicious commands through an unremoved ADOdb test page parameter, thereby executing arbitrary system commands on th

9.8 **CVE-2026-28165**

Unauthenticated Privilege Escalation in Digits <= 9.2 versions.

9.8 **CVE-2026-32558**

Unauthenticated Privilege Escalation in Affiliate Pro - Affiliate Program for WooCommerce & WordPress <= 8.9.1 versions.

9.8 **CVE-2026-66587**

Unauthenticated Local File Inclusion in WP Cafe Pro < 3.0.15 versions.

9.8 **CVE-2026-66648**

Unauthenticated Privilege Escalation in Jawn <= 1.4.2 versions.

9.8 **CVE-2026-66650**

Unauthenticated PHP Object Injection in FreightCo <= 1.1.15 versions.

9.8 **CVE-2026-76070**

+1 more CVEs in the same release

Netis NC63 firmware through V3.0.0.3327 contains a stack-based buffer overflow vulnerability that allows unauthenticated remote attackers to overwrite saved stack state by submitting an oversized Base64-encoded password to the login handler in /bin/netis.cgi.

9.8 **CVE-2026-71300** Apache camel

Improper input validation vulnerability in Apache Camel Atmosphere Websocket component. This issue affects Apache Camel: from 4.0.0 before 4.14.9, from 4.15.0 before 4.18.4, from 4.19.0 before 4.22.0. The camel-atmosphere-websocket producer selects which conne

9.8 **CVE-2026-77915**

rConfig Core 8.0.0 before 8.2.10 contains an authentication bypass vulnerability that allows unauthenticated attackers to self-register accounts with full Administrator privileges due to a duplicate bare Auth::routes() call in routes/web.php that re-enables th

9.8 **CVE-2026-78329** Apache camel

Improper input validation vulnerability in Apache Camel Undertow component. This issue affects Apache Camel: from 4.11.0 before 4.14.9, from 4.15.0 before 4.18.4, from 4.19.0 before 4.22.0. UndertowEndpoint defaulted its headerFilterStrategy field to the base

9.8 **CVE-2026-71914**

Multiple DrayTek VigorAP models contain a command injection vulnerability in the dray_apm component. The vulnerability is caused by insufficient validation of UDP message content after START_SPEED_TEST before command execution. A remote attacker can trigger th

9.8 **CVE-2026-71921**

Multiple DrayTek VigorSwitch models contain a pre-authentication command injection vulnerability in the setget.cgi interface. The vulnerability is caused by insufficient filtering of the pass field before command execution. A remote attacker can trigger this v

9.8 **CVE-2026-52490**

An issue in libtiff 85f2ac8e0b01cb7db2bbecf4a3b891bdbef67938 allows an attacker to execute arbitrary code via the process_command_opts() function in tools/tiffcrop.c

25 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.