Daily brief, Wednesday, November 19, 2025

Nov 18, 7:00 PM to Nov 19, 7:00 PM ET

Generated Nov 9, 2026, 8:23 AM ET

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

1 newly exploited, 18 new critical CVEs.

Breaking

Nothing spreading fast in technology large companies run.

Newly exploited in the wild

1

8.8 **CVE-2025-13223** Google Chromium V8 CISA KEV

A type confusion flaw in the Google Chromium V8 JavaScript engine lets an attacker corrupt the heap.

New public exploit code

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

New critical CVEs

18

9.8 **CVE-2025-13315** Lynxtechnology twonky server DETECTION

Twonky Server 8.5.2 on Linux and Windows is vulnerable to an access control flaw. An unauthenticated attacker can bypass web service API authentication controls to leak a log file and read the administrator's username and encrypted password.

9.8 **CVE-2025-63207** Rvr tex30lcdVs firmware DETECTION

The R.V.R Elettronica TEX product (firmware TEXL-000400, Web GUI TLAN-000400) is vulnerable to broken access control due to improper authentication checks on the /_Passwd.html endpoint. An attacker can send an unauthenticated POST request to change the Admin,

9.8 **CVE-2025-34329** Audiocodes fax server

AudioCodes Fax Server and Auto-Attendant IVR appliances versions up to and including 2.6.23 expose an unauthenticated backup upload endpoint at AudioCodes_files/ajaxBackupUploadFile.php in the F2MAdmin web interface. The script derives a backup folder path fro

9.8 **CVE-2025-63213** Qvidium opera11 firmware

The QVidium Opera11 device (firmware version 2.9.0-Ax4x-opera11) is vulnerable to Remote Code Execution (RCE) due to improper input validation on the /cgi-bin/net_ping.cgi endpoint. An attacker can exploit this vulnerability by sending a specially crafted GET

9.8 **CVE-2025-63223** Axeltechnology streamermax mk ii firmware

The Axel Technology StreamerMAX MK II devices (firmware versions 0.8.5 to 1.0.3) are vulnerable to Broken Access Control due to missing authentication on the /cgi-bin/gstFcgi.fcgi endpoint. Unauthenticated remote attackers can list user accounts, create new ad

9.8 **CVE-2025-34328** Audiocodes fax server

AudioCodes Fax Server and Auto-Attendant IVR appliances versions up to and including 2.6.23 include a web administration component (F2MAdmin) that exposes an unauthenticated script-management endpoint at AudioCodes_files/utils/IVR/diagram/ajaxScript.php. The s

10.0 **CVE-2025-63224** Itel idenc firmware

The Itel DAB Encoder (IDEnc build 25aec8d) is vulnerable to Authentication Bypass due to improper JWT validation across devices. Attackers can reuse a valid JWT token obtained from one device to authenticate and gain administrative access to any other device r

9.8 **CVE-2025-63218** Axeltechnology wolf1ms firmware

The Axel Technology WOLF1MS and WOLF2MS devices (firmware versions 0.8.5 to 1.0.3) are vulnerable to Broken Access Control due to missing authentication on the /cgi-bin/gstFcgi.fcgi endpoint. Unauthenticated remote attackers can list user accounts, create new

9.8 **CVE-2025-12057**

The WavePlayer WordPress plugin before 3.8.0 does not have authorization in an AJAX action as well as does not validate the file to be copied locally, allowing unauthenticated users to upload arbitrary file on the server and lead to RCE

9.8 **CVE-2025-63210** Newtec celoxa504 firmware

The Newtec Celox UHD (models: CELOXA504, CELOXA820) running firmware version celox-21.6.13 is vulnerable to an authentication bypass. An attacker can exploit this issue by modifying intercepted responses from the /celoxservice endpoint. By injecting a forged r

9.8 **CVE-2025-63206** Dasannetworks ds2924 firmware

An authentication bypass issue was discovered in Dasan Switch DS2924 web based interface, firmware versions 1.01.18 and 1.02.00, allowing attackers to gain escalated privileges via storing crafted cookies in the web browser.

9.1 **CVE-2025-63221** Axeltechnology puma firmware

The Axel Technology puma devices (firmware versions 0.8.5 to 1.0.3) are vulnerable to Broken Access Control due to missing authentication on the /cgi-bin/gstFcgi.fcgi endpoint. Unauthenticated remote attackers can list user accounts, create new administrative

9.8 **CVE-2025-65099** Anthropic claude code

Claude Code is an agentic coding tool. Prior to version 1.0.39, when running on a machine with Yarn 3.0 or above, Claude Code could have been tricked to execute code contained in a project via yarn plugins before the user accepted the startup trust dialog. Exp

9.1 **CVE-2025-65021** Rallly rallly

Rallly is an open-source scheduling and collaboration tool. Prior to version 4.5.4, an Insecure Direct Object Reference (IDOR) vulnerability exists in the poll finalization feature of the application. Any authenticated user can finalize a poll they do not own

9.4 **CVE-2025-65095**

Lookyloo is a web interface that allows users to capture a website page and then display a tree of domains that call each other. Prior to version 1.35.1, there is potential cross-site scripting on index and tree page. This issue has been patched in version 1.3

9.3 **CVE-2025-12592**

Legacy Vivotek Device firmware uses default credetials for the root and user login accounts.

9.8 **CVE-2025-10437**

Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in Eksagate Electronic Engineering and Computer Industry Trade Inc. Webpack Management System allows SQL Injection. This issue affects Webpack Management System:

9.3 **CVE-2025-13051**

When the service of ABP and AES is installed in a directory writable by non-administrative users, an attacker can replace or plant a DLL with the same name as one loaded by the service. Upon service restart, the malicious DLL is loaded and executed under the L

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. Leak-site data: RansomLook (ransomlook.io), CC BY 4.0; sectors grouped and countries mapped by Watch Floor. CVE IDs link to the full record on Watch Floor.