Daily brief, Tuesday, December 2, 2025

Dec 1, 7:00 PM to Dec 2, 7:00 PM ET

Generated Nov 9, 2026, 6:23 AM ET

0	2	0	27	0	0
Breaking	Newly exploited	Exploit code	Critical CVEs	Ransomware posts	New breaches

2 newly exploited, 27 new critical CVEs.

Breaking

Nothing spreading fast in technology large companies run.

Newly exploited in the wild

2

7.8 **CVE-2025-48572** Android Framework CISA KEV

An unspecified flaw in the Android Framework allows privilege escalation, giving an attacker elevated rights on affected Android devices.

5.5 **CVE-2025-48633** Android Framework CISA KEV

An unspecified flaw in the Android Framework lets an attacker disclose information; the input does not state the attack prerequisites.

New public exploit code

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

New critical CVEs

27

9.8 **CVE-2025-11779** Circutor sge-plc1000 firmware

Stack-based buffer overflow vulnerability in CircutorSGE-PLC1000/SGE-PLC50 v9.0.2. The 'SetLan' function is invoked when a new configuration is applied. This new configuration function is activated by a management web request, which can be invoked by a user wh

9.8 **CVE-2025-60854** Dlink r15 firmware

A vulnerability has been found in D-Link R15 (AX1500) 1.20.01 and below. By manipulating the model name parameter during a password change request in the web administrator page, it is possible to trigger a command injection in httpd.

9.8 **CVE-2025-59693** Entrust nshield 5c firmware

The Chassis Management Board in Entrust nShield Connect XC, nShield 5c, and nShield HSMi through 13.6.11, or 13.7 (patched in 13.6.12 (LTS) and 13.9.0 (STS)), allows a physically proximate attacker to obtain debug access and escalate privileges by bypassing th

9.3 **CVE-2025-13658**

A vulnerability in Longwatch devices allows unauthenticated HTTP GET requests to execute arbitrary code via an exposed endpoint, due to the absence of code signing and execution controls. Exploitation results in SYSTEM-level privileges.

9.8 **CVE-2025-59695** Entrust nshield 5c firmware

+1 more CVEs in the same release

Entrust nShield Connect XC, nShield 5c, and nShield HSMi through 13.6.11, or 13.7 (patched in 13.6.12 (LTS) and 13.9.0 (STS)), allow a user with OS root access to alter firmware on the Chassis Management Board (without Authentication). This is called F04.

9.1 **CVE-2025-66409** Espressif esp-idf

ESF-IDF is the Espressif Internet of Things (IOT) Development Framework. In 5.5.1, 5.4.3, 5.3.4, 5.2.6, 5.1.6, and earlier, when AVRCP is enabled on ESP32, receiving a malformed VENDOR DEPENDENT command from a peer device can cause the Bluetooth stack to acces

9.3 **CVE-2025-13510**

The Iskra iHUB and iHUB Lite smart metering gateway exposes its web management interface without requiring authentication, allowing unauthenticated users to access and modify critical device settings.

9.8 **CVE-2025-11783** Circutor sge-plc1000 firmware

Stack-based buffer overflow vulnerability in Circutor SGE-PLC1000/SGE-PLC50 v9.0.2. The vulnerability is found in the 'AddEvent()' function when copying the user-controlled username input to a fixed-size buffer (48 bytes) without boundary checking. This can le

9.8 **CVE-2025-60736** Anisha online medicine guide

code-projects Online Medicine Guide 1.0 is vulnerable to SQL Injection in /login.php via the upass parameter.

9.8 **CVE-2025-65656** Dcatadmin dcat admin

dcat-admin v2.2.3-beta and before is vulnerable to file inclusion in admin/src/Extend/VersionManager.php.

9.8 **CVE-2025-41742** Sprecher-Automation sprecon-e-c firmware

Sprecher Automations SPRECON-E-C, SPRECON-E-P, SPRECON-E-T3 is vulnerable to attack by an unauthorized remote attacker via default cryptographic keys. The use of these keys allows the attacker to read, modify, and write projects and data, or to access any devi

9.8 **CVE-2025-65896** Long2ice asyncmy

SQL injection vulnerability in long2ice assyncmy thru 0.2.10 allows attackers to execute arbitrary SQL commands via crafted dict keys.

9.1 **CVE-2025-41744** Sprecher-Automation sprecon-e-c firmware

Sprecher Automations SPRECON-E series uses default cryptographic keys that allow an unprivileged remote attacker to access all encrypted communications, thereby compromising confidentiality and integrity.

9.8 **CVE-2025-65358** Hashenudara edoc-doctor-appointment-system

Edoc-doctor-appointment-system v1.0.1 was discovered to contain SQl injection vulnerability via the 'docid' parameter at /admin/appointment.php.

9.8 **CVE-2025-11782** Circutor sge-plc1000 firmware

Stack-based buffer overflow vulnerability in Circutor SGE-PLC1000/SGE-PLC50 v9.0.2. The 'ShowDownload()' function uses “sprintf()” to format a string that includes the user-controlled input of 'GetParameter(meter)' in the fixed-size buffer 'acStack_4c' (64 byt

9.8 **CVE-2025-11784** Circutor sge-plc1000 firmware

Stack-based buffer overflow vulnerability in Circutor SGE-PLC1000/SGE-PLC50 v9.0.2. In the 'ShowMeterDatabase()' function, there is an unlimited user input that is copied to a fixed-size buffer via 'sprintf()'. The 'GetParameter(meter)' function retrieves the

9.8 **CVE-2025-11785** Circutor sge-plc1000 firmware

Stack-based buffer overflow vulnerability in Circutor SGE-PLC1000/SGE-PLC50 v9.0.2. In the 'ShowMeterPasswords()' function, there is an unlimited user input that is copied to a fixed-size buffer via 'sprintf()'. The 'GetParameter(meter)' function retrieves the

9.8 **CVE-2025-11786** Circutor sge-plc1000 firmware

Stack-based buffer overflow vulnerability in Circutor SGE-PLC1000/SGE-PLC50 v9.0.2. In the 'SetUserPassword()' function, the 'newPassword' parameter is directly embedded in a shell command string using 'sprintf()' without any sanitisation or validation, and th

9.8 **CVE-2025-13542**

The DesignThemes LMS plugin for WordPress is vulnerable to Privilege Escalation in all versions up to, and including, 1.0.4. This is due to the 'dtlms_register_user_front_end' function not restricting what user roles a user can register with. This makes it pos

9.8 **CVE-2025-11778** Circutor sge-plc1000 firmware

Stack-based buffer overflow in Circutor SGE-PLC1000/SGE-PLC50 v0.9.2. This vulnerability allows an attacker to remotely exploit memory corruption through the 'read_packet()' function of the TACACSPLUS implementation.

6 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. 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.