Daily brief, Saturday, December 13, 2025

Dec 12, 7:00 PM to Dec 13, 7:00 PM ET

Generated Nov 9, 2026, 4:41 AM ET

0	0	0	8	0	0
Breaking	Newly exploited	Exploit code	Critical CVEs	Ransomware posts	New breaches

8 new critical CVEs.

Breaking

Nothing spreading fast in technology large companies run.

Newly exploited in the wild

No CVEs added to CISA's known-exploited list.

New public exploit code

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

New critical CVEs

8

9.8 **CVE-2025-11693** DETECTION

The Export WP Page to Static HTML & PDF plugin for WordPress is vulnerable to Sensitive Information Exposure in all versions up to, and including, 4.3.4 through publicly exposed cookies.txt files containing authentication cookies. This makes it possible for un

9.8 **CVE-2025-14440**

The JAY Login & Register plugin for WordPress is vulnerable to authentication bypass in versions up to, and including, 2.4.01. This is due to incorrect authentication checking in the 'jay_login_register_process_switch_back' function with the 'jay_login_registe

9.8 **CVE-2025-10738**

The URL Shortener Plugin For WordPress plugin for WordPress is vulnerable to SQL Injection via the ‘analytic_id’ parameter in all versions up to, and including, 3.0.7 due to insufficient escaping on the user supplied parameter and lack of sufficient preparatio

9.8 **CVE-2025-36747** Growatt shine lan-x firmware

ShineLan-X contains a set of credentials for an FTP server was found within the firmware, allowing testers to establish an insecure FTP connection with the server. This may allow an attacker to replace legitimate files being deployed to devices with their own

9.8 **CVE-2025-36752** Growatt shine lan-x firmware

Growatt ShineLan-X communication dongle has an undocumented backup account with undocumented credentials which allows significant level access to the device, such as allowing any attacker to access the Setting Center. This means that this is effectively backdo

9.8 **CVE-2025-36753** Growatt shine lan-x firmware

The SWD debug interface on the Growatt ShineLan-X communication dongle is available by default, allowing an attacker to attain debug access to the device and to extracting secrets or domains from within the device

9.3 **CVE-2025-36754**

The authentication mechanism on web interface is not properly implemented. It is possible to bypass authentication checks by crafting a post request with new settings since there is no session token or authentication in place. This would allow an attacker for

9.4 **CVE-2025-36751**

Encryption is missing on the configuration interface for Growatt ShineLan-X and MIC 3300TL-X. This allows an attacker with access to the network to intercept and potentially manipulate communication requests between the inverter and its cloud endpoint.

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.