Daily brief, Monday, November 24, 2025

Nov 23, 7:00 PM to Nov 24, 7:00 PM ET

Generated Nov 9, 2026, 7:37 AM ET

0	0	0	7	0	0
Breaking	Newly exploited	Exploit code	Critical CVEs	Ransomware posts	New breaches

7 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

7

9.8 **CVE-2024-47856** Rsa authentication agent for windows

In RSA Authentication Agent before 7.4.7, service paths and shortcut paths may be vulnerable to path interception if the path has one or more spaces and is not surrounded by quotation marks. An adversary can place an executable in a higher-level directory of t

9.3 **CVE-2018-25126**

Shenzhen TVT Digital Technology Co., Ltd. NVMS-9000 firmware (used by many white-labeled DVR/NVR/IPC products) contains hardcoded API credentials and an OS command injection flaw in its configuration services. The web/API interface accepts HTTP/XML requests au

9.9 **CVE-2025-54347** Desktopalert pingalert application server

A Directory Traversal vulnerability was found in the Application Server of Desktop Alert PingAlert version 6.1.0.11 to 6.1.1.2 which allows an attacker to write arbitrary files under certain conditions.

9.1 **CVE-2025-12977** Treasuredata fluent bit

Fluent Bit in_http, in_splunk, and in_elasticsearch input plugins fail to sanitize tag_key inputs. An attacker with network access or the ability to write records into Splunk or Elasticsearch can supply tag_key values containing special characters such as newl

9.3 **CVE-2023-7330**

Ruijie NBR series routers contain an unauthenticated arbitrary file upload vulnerability via /ddi/server/fileupload.php. The endpoint accepts attacker-supplied values in the name and uploadDir parameters and saves the provided multipart file content without ad

9.8 **CVE-2025-63958** Millensys vision tools workspace

MILLENSYS Vision Tools Workspace 6.5.0.2585 exposes a sensitive configuration endpoint (/MILLENSYS/settings) that is accessible without authentication. This page leaks plaintext database credentials, file share paths, internal license server configuration, and

9.8 **CVE-2025-40212**

In the Linux kernel, the following vulnerability has been resolved: nfsd: fix refcount leak in nfsd_set_fh_dentry() nfsd exports a "pseudo root filesystem" which is used by NFSv4 to find the various exported filesystems using LOOKUP requests from a known root

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.