Daily brief, Wednesday, February 11, 2026

Feb 10, 7:00 PM to Feb 11, 7:00 PM ET

Generated Nov 7, 2026, 6:04 PM ET

0	0	0	24	0	0
Breaking	Newly exploited	Exploit code	Critical CVEs	Ransomware posts	New breaches

24 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

24

9.0 **CVE-2026-20677** Apple ipados

A race condition was addressed with improved handling of symbolic links. This issue is fixed in iOS 18.7.5 and iPadOS 18.7.5, iOS 26.3 and iPadOS 26.3, macOS Sequoia 15.7.4, macOS Sonoma 14.8.4, macOS Tahoe 26.3, visionOS 26.3. A shortcut may be able to bypass

9.8 **CVE-2026-1357** DETECTION

The Migration, Backup, Staging – WPvivid Backup & Migration plugin for WordPress is vulnerable to Unauthenticated Arbitrary File Upload in versions up to and including 0.9.123. This is due to improper error handling in the RSA decryption process combined with

9.8 **CVE-2020-37153** Inextrix astpp

ASTPP 4.0.1 contains multiple vulnerabilities including cross-site scripting and command injection in SIP device configuration and plugin management interfaces. Attackers can exploit these flaws to inject system commands, hijack administrator sessions, and pot

9.8 **CVE-2026-25994** Pjsip pjsip

PJSIP is a free and open source multimedia communication library written in C. In 2.16 and earlier, a buffer overflow vulnerability exists in PJNATH ICE Session when processing credentials with excessively long usernames.

9.8 **CVE-2020-37186**

Chevereto 3.13.4 Core contains a remote code execution vulnerability that allows attackers to inject malicious code during database configuration installation. Attackers can manipulate the database table prefix parameter to write a PHP shell file and execute a

9.3 **CVE-2026-26215**

manga-image-translator version beta-0.3 and prior in shared API mode contains an unsafe deserialization vulnerability that can lead to unauthenticated remote code execution. The FastAPI endpoints /simple_execute/{method} and /execute/{method} deserialize attac

9.8 **CVE-2025-69874** Unjs nanotar

nanotar through 0.2.0 has a path traversal vulnerability in parseTar() and parseTarGzip() that allows remote attackers to write arbitrary files outside the intended extraction directory via a crafted tar archive containing path traversal sequence.

10.0 **CVE-2025-64075**

A path traversal vulnerability in the check_token function of Shenzhen Zhibotong Electronics ZBT WE2001 23.09.27 allows remote attackers to bypass authentication and perform administrative actions by supplying a crafted session cookie value.

9.8 **CVE-2026-25084**

Authentication for ZLAN5143D can be bypassed by directly accessing internal URLs.

9.8 **CVE-2026-24789**

An unprotected API endpoint allows an attacker to remotely change the device password without providing authentication.

9.8 **CVE-2025-66277** Qnap qts

A link following vulnerability has been reported to affect several QNAP operating system versions. The remote attackers can then exploit the vulnerability to traverse the file system to unintended locations. We have already fixed the vulnerability in the follo

9.8 **CVE-2025-70085** Opensatkit opensatkit

An issue was discovered in OpenSatKit 2.2.1. The EventErrStr buffer has a fixed size of 256 bytes. The code uses sprintf to format two filenames (Source1Filename and the string returned by FileUtil_FileStateStr) into this buffer without any length checking and

9.8 **CVE-2025-69872**

DiskCache (python-diskcache) through 5.6.3 uses Python pickle for serialization by default. An attacker with write access to the cache directory can achieve arbitrary code execution when a victim application reads from the cache.

9.8 **CVE-2026-2248**

METIS WIC devices (versions <= oscore 2.1.234-r18) expose a web-based shell at the /console endpoint that does not require authentication. Accessing this endpoint allows a remote attacker to execute arbitrary operating system commands with root (UID 0) privile

9.8 **CVE-2026-2249**

METIS DFS devices (versions <= oscore 2.1.234-r18) expose a web-based shell at the /console endpoint that does not require authentication. Accessing this endpoint allows a remote attacker to execute arbitrary operating system commands with 'daemon' privileges.

9.8 **CVE-2025-8025**

Missing Authentication for Critical Function, Improper Access Control vulnerability in Dinosoft Business Solutions Dinosoft ERP allows Accessing Functionality Not Properly Constrained by ACLs. This issue affects Dinosoft ERP: from < 3.0.1 through 11022026. NOT

9.8 **CVE-2026-26021** Set-In Project set-in

set-in provides the set value of nested associative structure given array of keys. A prototype pollution vulnerability exists in the the npm package set-in (>=2.0.1, < 2.0.5). Despite a previous fix that attempted to mitigate prototype pollution by checking wh

9.8 **CVE-2020-37176**

Torrent 3GP Converter 1.51 contains a stack overflow vulnerability that allows attackers to execute arbitrary code by overwriting Structured Exception Handler (SEH) registers. Attackers can craft a malicious payload targeting the application's registration dia

9.8 **CVE-2020-37181**

Torrent FLV Converter 1.51 Build 117 contains a stack overflow vulnerability that allows attackers to overwrite Structured Exception Handler (SEH) through a malicious registration code input. Attackers can craft a payload with specific offsets and partial SEH

9.8 **CVE-2020-37183**

Allok RM RMVB to AVI MPEG DVD Converter 3.6.1217 contains a stack overflow vulnerability that allows attackers to execute arbitrary code by overwriting Structured Exception Handler (SEH) registers. Attackers can craft a malicious payload in the License Name in

4 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.