Daily brief, Thursday, February 5, 2026

Feb 4, 7:00 PM to Feb 5, 7:00 PM ET

Generated Nov 7, 2026, 7:05 PM ET

0	2	0	14	0	1
Breaking	Newly exploited	Exploit code	Critical CVEs	Ransomware posts	New breaches

2 newly exploited, 14 new critical CVEs, 1 new breaches.

Breaking

Nothing spreading fast in technology large companies run.

Newly exploited in the wild

2

9.3 **CVE-2026-24423** SmarterTools SmarterMail CISA KEV DETECTION

Attacker gets OS command execution in SmarterTools SmarterMail by redirecting the unauthenticated ConnectToHub API to a malicious HTTP server serving commands.

9.8 **CVE-2025-11953** React Native Community CLI CISA KEV DETECTION

CVE published Nov 3, 2025

Unauthenticated network attackers can send POST requests to the React Native Community CLI Metro Dev Server to execute arbitrary OS commands.

New public exploit code

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

New critical CVEs

14

9.3 **CVE-2026-24423** SmarterTools SmarterMail KEV EXPLOIT CODE DETECTION

Attacker gets OS command execution in SmarterTools SmarterMail by redirecting the unauthenticated ConnectToHub API to a malicious HTTP server serving commands.

9.8 **CVE-2026-24300** Microsoft azure front door

Azure Front Door Elevation of Privilege Vulnerability

10.0 **CVE-2025-68121** Golang go

During session resumption in crypto/tls, if the underlying Config has its ClientCAs or RootCAs fields mutated between the initial handshake and the resumed handshake, the resumed handshake may succeed when it should have failed. This may happen when a user cal

9.3 **CVE-2026-0106** Google android

In vpu_mmap of vpu_ioctl, there is a possible arbitrary address mmap due to a missing bounds check. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.

9.8 **CVE-2020-37125** Edimax ew-7438rpn mini firmware

Edimax EW-7438RPn-v3 Mini 1.27 contains a remote code execution vulnerability that allows unauthenticated attackers to execute arbitrary commands through the /goform/mp endpoint. Attackers can exploit the vulnerability by sending crafted POST requests with com

9.8 **CVE-2020-37123** DETECTION

Pinger 1.0 contains a remote code execution vulnerability that allows attackers to inject shell commands through the ping and socket parameters. Attackers can exploit the unsanitized input in ping.php to write arbitrary PHP files and execute system commands by

9.8 **CVE-2020-37119** Nsasoft nsauditor

Nsauditor 3.0.28 and 3.2.1.0 contains a buffer overflow vulnerability in the DNS Lookup tool that allows attackers to execute arbitrary code by overwriting memory. Attackers can craft a malicious DNS query payload to trigger a three-byte overwrite, bypass ASLR

9.8 **CVE-2020-37138**

10-Strike Network Inventory Explorer 9.03 contains a buffer overflow vulnerability in the file import functionality that allows remote attackers to execute arbitrary code. Attackers can craft a malicious text file with carefully constructed payload to trigger

9.8 **CVE-2020-37126**

Free Desktop Clock 3.0 contains a stack overflow vulnerability in the Time Zones display name input that allows attackers to overwrite Structured Exception Handler (SEH) registers. Attackers can exploit the vulnerability by crafting a malicious Unicode input t

9.8 **CVE-2020-37120**

Rubo DICOM Viewer 2.0 contains a buffer overflow vulnerability in the DICOM server name input field that allows attackers to overwrite Structured Exception Handler (SEH). Attackers can craft a malicious text file with carefully constructed payload to execute a

9.8 **CVE-2020-37124**

B64dec 1.1.2 contains a buffer overflow vulnerability that allows attackers to execute arbitrary code by overwriting Structured Exception Handler (SEH) with crafted input. Attackers can leverage an egg hunter technique and carefully constructed payload to inje

9.8 **CVE-2020-37129**

Memu Play 7.1.3 contains an insecure folder permissions vulnerability that allows low-privileged users to modify the MemuService.exe executable. Attackers can replace the service executable with a malicious file during system restart to gain SYSTEM-level privi

9.8 **CVE-2026-23796** Opensolution quick.cart

Quick.Cart allows a user's session identifier to be set before authentication. The value of this session ID stays the same after authentication. This behaviour enables an attacker to fix a session ID for a victim and later hijack the authenticated session. The

9.0 **CVE-2025-68723** Axigen axigen mail server

Axigen Mail Server before 10.5.57 contains multiple stored Cross-Site Scripting (XSS) vulnerabilities in the WebAdmin interface. Three instances exist: (1) the log file name parameter in the Local Services Log page, (2) certificate file content in the SSL Cert

Ransomware

No leak-site posts collected.

New data breaches 1

Betterment betterment.com FINANCE 1,435,174 accounts

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.