Daily brief, Monday, March 2, 2026

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

Generated Nov 7, 2026, 3:04 PM ET

0	0	0	48	0	3
Breaking	Newly exploited	Exploit code	Critical CVEs	Ransomware posts	New breaches

48 new critical CVEs, 3 new breaches.

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

48

9.8 **CVE-2026-0006** Google android

In multiple locations, there is a possible out of bounds read and write due to a heap buffer overflow. This could lead to remote code execution with no additional execution privileges needed. User interaction is not needed for exploitation.

9.1 **CVE-2025-48609** Google android

In multiple functions of MmsProvider.java, there is a possible way to arbitrarily delete files which affect telephony, SMS, and MMS functionalities due to a path traversal error. This could lead to local denial of service with no additional execution privilege

9.8 **CVE-2025-48645** Google android

In loadDescription of DeviceAdminInfo.java, there is a possible persistent package due to improper input validation. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitatio

9.8 **CVE-2026-24107** Tenda w20e firmware

An issue was discovered in Tenda W20E V4.0br_V15.11.0.6. Failure to validate the value of `usbPartitionName`, which is directly used in `doSystemCmd`, may lead to critical command injection vulnerabilities.

9.8 **CVE-2026-24105** Tenda ac15 firmware

An issue was discovered in goform/formsetUsbUnload in Tenda AC15V1.0 V15.03.05.18_multi. The value of `v1` was not checked, potentially leading to a command injection vulnerability if injected into doSystemCmd.

9.8 **CVE-2026-24101** Tenda ac15 firmware

An issue was discovered in goform/formSetIptv in Tenda AC15V1.0 V15.03.05.18_multi. When the condition is met, `s1_1` will be passed into sub_B0488, concatenated into `doSystemCmd`. The value of s1_1 is not validated, potentially leading to a command injection

9.8 **CVE-2026-23600** Hpe autopass license server

A remote authentication bypass vulnerability exists in HPE AutoPass License Server (APLS).

9.8 **CVE-2025-50187** Chamilo chamilo lms

Chamilo is a learning management system. Prior to version 1.11.28, parameter from SOAP request is evaluated without filtering which leads to Remote Code Execution. This issue has been patched in version 1.11.28.

9.8 **CVE-2026-26720** Twenty twenty

An issue in Twenty CRM v1.15.0 and before allows a remote attacker to execute arbitrary code via the local.driver.ts module.

9.8 **CVE-2026-3422** Edetw u-office force

U-Office Force developed by e-Excellence has a Insecure Deserialization vulnerability, allowing unauthenticated remote attackers to execute arbitrary code on the server by sending maliciously crafted serialized content.

9.8 **CVE-2026-24115** Tenda w20e firmware

An issue was discovered in Tenda W20E V4.0br_V15.11.0.6. Failure to validate the sizes of `gstup` and `gstdwn` before concatenating them into `gstruleQos` may lead to buffer overflow.

9.8 **CVE-2026-24108** Tenda w20e firmware

+2 more CVEs in the same release

An issue was discovered in Tenda W20E V4.0br_V15.11.0.6. Attackers may exploit the vulnerability by controlling the value of `nptr`. When this value is passed into the `getMibPrefix` function and concatenated using `sprintf` without proper size validation, it

9.8 **CVE-2026-24111** Tenda w20e firmware

+1 more CVEs in the same release

An issue was discovered in Tenda W20E V4.0br_V15.11.0.6. Attackers may exploit the vulnerability by specifying the value of `userInfo`. When `userInfo` is passed into the `addAuthUser` function and processed by `sscanf` without size validation, it could lead t

9.8 **CVE-2026-24114** Tenda w20e firmware

An issue was discovered in Tenda W20E V4.0br_V15.11.0.6. Failure to validate `pPortMapIndex` may lead to buffer overflows when using `strcpy`.

9.8 **CVE-2025-50190** Chamilo chamilo lms

Chamilo is a learning management system. Prior to version 1.11.30, there is an error-based SQL Injection via the GET openid.assoc_handle parameter with the /index.php script. This issue has been patched in version 1.11.30.

9.8 **CVE-2025-50192** Chamilo chamilo lms

Chamilo is a learning management system. Prior to version 1.11.30, there is a time-based SQL Injection in found in /main/webservices/registration.soap.php. This issue has been patched in version 1.11.30.

9.8 **CVE-2025-14532** Studiofabryka dorbycms

DobryCMS's upload file functionality allows an unauthenticated remote attacker to upload files of any type and extension without restriction, which can result in Remote Code Execution. This issue was fixed in versions above 5.0.

9.8 **CVE-2026-26702** Jon-Remus-Sevellejo personnel property equipment system

sourcecodester Personnel Property Equipment System v1.0 is vulnerable to SQL Injection in /ppes/admin/myitem_reuse.php.

9.8 **CVE-2026-26703** Jon-Remus-Sevellejo personnel property equipment system

sourcecodester Personnel Property Equipment System v1.0 is vulnerable to SQL Injection in /ppes/admin/advance_search.php.

9.4 **CVE-2025-30044**

In the endpoints "/cgi-bin/CliniNET.prd/utils/usrlogstat_simple.pl", "/cgi-bin/CliniNET.prd/utils/usrlogstat.pl", "/cgi-bin/CliniNET.prd/utils/userlogstat2.pl", and "/cgi-bin/CliniNET.prd/utils/dblogstat.pl", the parameters are not sufficiently normalized, whi

25 more critical CVEs in this window: see the dashboard

Ransomware

No leak-site posts collected.

New data breaches 3

KomikoAI komiko.app	1,060,191 accounts
Lovora	495,556 accounts
Quitbro quitbro.app	22,874 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.