Daily brief, Monday, July 13, 2026

Jul 12, 8:00 PM to Jul 13, 8:00 PM ET

Generated Nov 3, 2026, 7:17 PM ET

0	1	0	51	0	0
Breaking	Newly exploited	Exploit code	Critical CVEs	Ransomware posts	New breaches

1 newly exploited, 51 new critical CVEs.

Breaking

Nothing spreading fast in technology large companies run.

Newly exploited in the wild

1

8.1 **CVE-2008-4128** Cisco IOS CISA KEV

An attacker can execute arbitrary commands on a Cisco IOS server via cross-site request forgery.

New public exploit code

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

New critical CVEs

51

10.0 **CVE-2026-57719**

Unrestricted Upload of File with Dangerous Type vulnerability in CodeRevolution Aimogen Pro aimogen-pro allows Using Malicious Files.This issue affects Aimogen Pro: from n/a through <= 2.8.3.

10.0 **CVE-2026-57811**

Improper Control of Generation of Code ('Code Injection') vulnerability in Realtyna Realtyna Organic IDX plugin real-estate-listing-realtyna-wpl allows Remote Code Inclusion.This issue affects Realtyna Organic IDX plugin: from n/a through <= 5.2.0.

9.9 **CVE-2026-57401**

Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal') vulnerability in Brainstorm Force SureDash suredash allows Path Traversal.This issue affects SureDash: from n/a through <= 1.8.0.

9.9 **CVE-2026-57710**

Unrestricted Upload of File with Dangerous Type vulnerability in quantumcloud WoowBot Pro Max woowbot-pro-max allows Using Malicious Files.This issue affects WoowBot Pro Max: from n/a through <= 14.1.7.

9.8 **CVE-2026-4769**

Certain devices in the WAGO System I/O Field series activate an internal diagnostic capability during the initial startup sequence. This functionality is not formally documented and becomes accessible without authentication for a brief period in the early boot

9.8 **CVE-2026-57724**

Deserialization of Untrusted Data vulnerability in Themeum Kirki kirki allows Object Injection.This issue affects Kirki: from n/a through <= 6.0.12.

9.8 **CVE-2026-57738**

Deserialization of Untrusted Data vulnerability in axiomthemes 777 triple-seven allows Object Injection.This issue affects 777: from n/a through <= 1.13.0.

9.8 **CVE-2026-57744**

Deserialization of Untrusted Data vulnerability in stmcan RT-Theme 18 | Extensions rt18-extensions allows Object Injection.This issue affects RT-Theme 18 | Extensions: from n/a through <= 2.5.

9.8 **CVE-2026-57770**

Deserialization of Untrusted Data vulnerability in ThemeGoods Grand Photography grandphotography allows Object Injection.This issue affects Grand Photography: from n/a through <= 5.7.8.

9.8 **CVE-2026-57813**

Incorrect Privilege Assignment vulnerability in properfraction MailOptin mailoptin allows Privilege Escalation.This issue affects MailOptin: from n/a through <= 1.2.77.3.

9.8 **CVE-2026-59518**

Deserialization of Untrusted Data vulnerability in wpWax Directorist directorist allows Object Injection.This issue affects Directorist: from n/a through <= 8.8.2.

9.8 **CVE-2026-60121** Vitec flamingo

Vitec Flamingo 4.12.2 contains an unauthenticated OS command injection vulnerability in the admin/ajax/ping.php endpoint that allows remote attackers to execute arbitrary commands by exploiting a double-evaluation flaw in shell argument handling. The endpoint

9.8 **CVE-2026-61498** Vitec flamingo

Vitec Flamingo 4.12.2 contains an unauthenticated OS command injection vulnerability in the admin/ajax/gen_graphs.php endpoint that allows remote unauthenticated attackers to execute arbitrary commands by supplying shell metacharacters in the start, end, key,

9.8 **CVE-2026-57433** Nwclark storable

Storable versions before 3.41 for Perl have a signed integer overflow when deserializing a crafted SX_HOOK record. retrieve_hook_common reads a signed 32-bit item count from an SX_HOOK record and calls av_extend with that count plus one. A count of I32_MAX wra

9.8 **CVE-2026-61500** DETECTION

Rejetto HFS 3.0.0 through 3.2.0 derives its session-cookie signing key from the non-cryptographic Math.random() generator and discloses outputs of the same generator to unauthenticated clients during login. A remote attacker can collect a small number of login

9.8 **CVE-2026-51540** Opener Project opener

OpENer 2.3.0 (master branch up to commit 76b95cf) is vulnerable to a severe memory corruption issue caused by an integer underflow in the processing of connected explicit messages (SendUnitData).

9.8 **CVE-2026-51821**

SQL Injection vulnerability in Shenzhou Shihan Video Conference System v.1.0 allows a remote attacker to execute arbitrary code via the /user/getUserLogin endpoint

9.8 **CVE-2026-52533**

An issue in D-Link DIR-1253 v.1.0.1.250923.142435 allows an attacker to escalate privileges via the etc/shadow component file

9.8 **CVE-2026-59801** DETECTION

9Router through version 0.4.41 contains an unauthenticated access vulnerability that allows remote attackers to interact with provider management API endpoints by sending requests without any credentials due to missing authentication middleware in the Next.js

9.6 **CVE-2026-14453**

This vulnerability is a critical Server-Side Template Injection (SSTI) in Centreon's centreon-open-tickets module that leads to Remote Code Execution. The message_confirm field is stored without sanitization and rendered via Smarty with no security policy enab

31 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. CVE IDs link to the full record on Watch Floor.