Daily brief, Wednesday, November 11, 2026

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

Generated Nov 11, 2026, 8:42 PM ET

4	0	3	40	37	2
Breaking	Newly exploited	Exploit code	Critical CVEs	Ransomware posts	New breaches

4 breaking, 3 emerging, 3 with new public exploit code, 40 new critical CVEs, 37 ransomware posts, 2 new breaches.

Breaking 4

Google Chrome: Memory corruption

- 20 posts from 20 independent sources in 48 h
- Chrome: very widely used in large enterprises
- remote code execution / auth bypass
- exploited in the wild (CISA KEV)
- public exploit code

CVEs: CVE-2026-125350

OpenBSD OpenSSH: Auth bypass / access control

- 13 posts from 12 independent sources in 48 h
- OpenSSH: very widely used in large enterprises
- auth bypass / access control
- exploited in the wild (CISA KEV)
- public exploit code
- official advisory

CVEs: CVE-2026-123158

PHP2Shell · PHP

- 23 posts from 8 independent sources in 48 h
- PHP: very widely used in large enterprises
- remote code execution / auth bypass
- exploited in the wild (CISA KEV)
- public exploit code
- official advisory

CVEs: CVE-2026-109618, CVE-2026-109619

Microsoft 365 apps

- 15 posts from 13 independent sources in 48 h
- rising: 15 posts in the last 24 h
- Windows: very widely used in large enterprises
- exploited in the wild (CISA KEV)
- public exploit code

CVEs: CVE-2026-124194

Emerging 3

Critical bugs in widely used enterprise tech, not spreading widely yet.

Cisco broadworks application delivery platform

- 4 posts from 4 independent sources in 48 h
- Cisco: very widely used in large enterprises
- exploited in the wild (CISA KEV)

CVEs: CVE-2026-20320

SAP SE SAP Gateway: Auth bypass / access control

- 4 posts from 4 independent sources in 48 h
- SAP: very widely used in large enterprises
- auth bypass / access control
- official advisory

CVEs: CVE-2026-89103

SonicWall SonicOS

- 3 posts from 3 independent sources in 48 h
- SonicWall: widely used in large enterprises
- exploited in the wild (CISA KEV)

CVEs: CVE-2026-19868

Newly exploited in the wild

No CVEs added to CISA's known-exploited list.

New public exploit code 3

9.8 **CVE-2026-123488** Craftcms cms NUCLEI TEMPLATE DETECTION
Unauthenticated remote attackers can inject stacked SQL via the attribute parameter of the element search endpoint in Craft CMS 4.x before 4.18.9 and 5.x before 5.11.2.

9.8 **CVE-2026-123270** Redpanda Data Connect NUCLEI TEMPLATE DETECTION
Unauthenticated remote code execution in Redpanda Connect 4.39-4.110 streams mode via the management HTTP API on port 4195, which has auth disabled by default.

5.3 **CVE-2026-62850** Freescout-Help-Desk freescout NUCLEI TEMPLATE DETECTION
Unauthenticated attackers can use FreeScout's tools.php maintenance endpoint (before 1.8.225) to learn whether arbitrary server directories exist.

3 older CVEs (published more than 7 days earlier) with new exploit code, below the bar (CVSS under 9, not widely used enterprise tech):
CVE-2026-92998 (8.6), CVE-2026-116747 (8.1), CVE-2026-19697 (6.8)

New critical CVEs 40

9.8 **CVE-2026-126170** Fortinet FortiOS EXPLOIT CODE
Improper output encoding or escaping flaw in Fortinet FortiAnalyzer 7.6 and 8.0 and FortiManager 8.0 releases; the truncated summary does not state the attacker impact or access required.

9.8 **CVE-2026-64678** Nitrite nitrite-java
Nitrite (nitrite-java) before 4.4.1 has an unsafe deserialization flaw (CWE-502) triggered automatically when a database file is opened during its legacy v1-format store check.

9.8 **CVE-2026-126147** Fortinet FortiMail
Path traversal in multiple Fortinet FortiMail 7.2, 7.4, 7.6 and 8.0 releases lets an unauthenticated attacker execute unauthorized code or commands.

9.8 **CVE-2026-126148** Fortinet FortiMail
An unauthenticated attacker executes arbitrary OS commands via crafted HA join-request packets in Fortinet FortiMail 8.0.0-8.0.1 and 7.6.0-7.6.6.

9.8 **CVE-2026-126259** Fortinet FortiOS
Unauthenticated attacker executes commands as super admin on FortiOS 7.2 to 8.0.0 in HA FGSP with standalone-config-sync or in autoscale deployments.

9.8 **CVE-2026-126262** Fortinet FortiAnalyzer
SQL injection in multiple Fortinet FortiAnalyzer 7.2-8.0 releases and FortiManager 8.0.0 lets an attacker inject SQL commands; the version list is truncated.

9.8 **CVE-2026-126263** Fortinet FortiMail
+1 more CVEs in the same release
An authenticated attacker can execute unauthorized code or commands through SQL injection in multiple Fortinet FortiMail 7.4, 7.6, and 8.0 releases.

9.6 **CVE-2026-126254** Fortinet FortiOS
A configured iBGP neighbor in affected Fortinet FortiOS 7.2 through 8.0.1 builds can send malformed attributes to all connected routers via a crafted request.

9.3 **CVE-2026-126253** Fortinet FortiOS
Authentication bypass in Fortinet FortiOS 7.2.0 through 8.0.1 lets an unauthenticated attacker broadcast LSA packets via a specially crafted request.

9.1 **CVE-2026-126150** Fortinet FortiMail
An unauthenticated attacker can reset the password of any IBE webmail user on affected Fortinet FortiMail releases, taking over that account.

9.1 **CVE-2026-126155** Fortinet FortiMail
Unauthenticated remote attacker gains authenticated IBE webmail session as any IBE recipient in Fortinet FortiMail 7.2, 7.4.0-7.4.8, 7.6.0-7.6.6, 8.0.0-8.0.1.

9.1 **CVE-2026-126156** Fortinet FortiMail
Unauthenticated remote attackers can take over arbitrary IBE recipient accounts in multiple Fortinet FortiMail branches (7.2 to 8.0.1) via a user-controlled key authorization bypass.

9.1 **CVE-2026-126157** Fortinet FortiMail
Unauthenticated attackers gain access to other users' secure email accounts in Fortinet FortiMail 7.2, 7.4, 7.6 and 8.0 branches via crafted HTTP requests.

9.1 **CVE-2026-126229** Fortinet FortiManager
An authorization bypass via a user-controlled key in Fortinet FortiAnalyzer and FortiAnalyzer Cloud lets an attacker access resources beyond their permissions.

9.1 **CVE-2026-126251** Fortinet FortiAuthenticator
An incorrect authorization flaw in Fortinet FortiAuthenticator 8.0.0-8.0.3 and 6.6.0-6.6.10 lets an attacker bypass authentication and gain unauthorized access.

9.0 **CVE-2026-126257** Fortinet FortiAuthenticator
Unauthenticated attackers bypass credential validation via a hard-coded password in FortiAuthenticator 8.0.0–8.0.3 and 6.6.0–6.6.10, gaining unauthorized access.

10.0 **CVE-2026-78287** Staggs STAGGS
Code injection in Staggs STAGGS through version 3.3.0 lets an attacker include and execute remote code.

9.9 **CVE-2026-110697** Red Hat Red Hat OpenShift Update Service
Quay's robot account listing fails to escape LIKE wildcards in namespace names, letting an attacker who creates an underscore-named namespace retrieve robot account data.

9.8 **CVE-2026-126542** WWBN AVideo
Unauthenticated attackers log in as any user of WWBN AVideo 6.5-29.7.1 by setting a Hybridauth social login display name to the victim's username.

9.8 **CVE-2026-64682** NauelG astro-blocks

AstroBlocks CMS before 3.4.0 lets attackers forge admin session tokens using a hard-coded fallback JWT secret readable in the published package.

19 more critical CVEs in this window: see the dashboard

Ransomware 37

37 victims posted to leak sites. Most active: the gentlemen (22), curious worm (9), akira (3), dark project (2), deadlock (1).

New data breaches 2

YouHack	youhack.ru		7,160,849 accounts
??????????? (SberSpasibo)	spasibosberbank.ru	FINANCE	3,288,711 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.