# Daily brief, Friday, September 11, 2026

Sep 10, 8:00 PM to Sep 11, 8:00 PM ET

Generated Nov 1, 2026, 10:14 AM ET

| 0 | 4 | 0 | 4 | 0 | 0 |
|---|---|---|---|---|---|
| Breaking | Newly exploited | Exploit code | Critical CVEs | Ransomware posts | New breaches |

4 newly exploited, 4 new critical CVEs.

## Breaking

*Nothing spreading fast in technology large companies run.*

## Newly exploited in the wild

4

**10.0** **CVE-2026-85706** GitLab Community Edition and Enterprise Edition CISA KEV DETECTION

An attacker can access sensitive files and data outside of the intended repository path on GitLab Community Edition and Enterprise Edition.

**9.9** **CVE-2026-84869** ConnectWise ScreenConnect CISA KEV

An attacker can transfer and execute files through a remote session on ConnectWise ScreenConnect without authentication.

**8.1** **CVE-2026-42016** JFrog Artifactory CISA KEV

An attacker can escalate privileges on a JFrog Artifactory server with incorrect authorization.

**7.5** **CVE-2026-42018** JFrog Artifactory CISA KEV DETECTION

An unauthenticated caller gets access to sensitive resources with JFrog Artifactory.

## New public exploit code

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

## New critical CVEs

4

**10.0** **CVE-2026-85706** GitLab Community Edition and Enterprise Edition KEV EXPLOIT CODE DETECTION

An attacker can access sensitive files and data outside of the intended repository path on GitLab Community Edition and Enterprise Edition.

9.9 **CVE-2026-84869** ConnectWise ScreenConnect KEV
An attacker can transfer and execute files through a remote session on ConnectWise ScreenConnect without authentication.

9.8 **CVE-2026-89010** WAVLINK Technology WN535M1 DETECTION
An attacker can execute arbitrary commands as root on WAVLINK WN535M1 routers.

9.1 **CVE-2026-89009** WAVLINK Technology WN535M1 DETECTION
A remote attacker can overwrite any file on a WAVLINK WN535M1 or WN535M3 router without authentication.

## 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.