Daily brief, Tuesday, March 17, 2026

Mar 16, 8:00 PM to Mar 17, 8:00 PM ET

Generated Nov 7, 2026, 12:48 PM ET

0	0	0	8	0	0
Breaking	Newly exploited	Exploit code	Critical CVEs	Ransomware posts	New breaches

8 new critical CVEs.

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

8

9.8 **CVE-2026-21994** Oracle okit

Vulnerability in the Oracle Edge Cloud Infrastructure Designer and Visualisation Toolkit product of Oracle Open Source Projects (component: Desktop). The supported version that is affected is 0.3.0. Easily exploitable vulnerability allows unauthenticated attac

9.1 **CVE-2026-25769** Wazuh wazuh

Wazuh is a free and open source platform used for threat prevention, detection, and response. Versions 4.0.0 through 4.14.2 have a Remote Code Execution (RCE) vulnerability due to Deserialization of Untrusted Data). All Wazuh deployments using cluster mode (ma

9.1 **CVE-2026-25770** Wazuh wazuh

Wazuh is a free and open source platform used for threat prevention, detection, and response. Starting in version 3.9.0 and prior to version 4.14.3, a privilege escalation vulnerability exists in the Wazuh Manager's cluster synchronization protocol. The `wazuh

9.1 **CVE-2026-32298** Angeet es3 kvm firmware

The Angeet ES3 KVM does not properly sanitize user-supplied variables parsed by the 'cfg.lua' script, allowing an authenticated attacker to execute OS-level commands.

9.8 **CVE-2026-4312** Dragonsoft gcb\/fcb government financial cybersecurity configuration audit software

GCB/FCB Audit Software developed by DrangSoft has a Missing Authentication vulnerability, allowing unauthenticated remote attackers to directly access certain APIs to create a new administrative account.

9.0 **CVE-2026-3564**

A condition in the ScreenConnect server component may allow an actor with access to server-level cryptographic material used for authentication to obtain unauthorized access, including elevated privileges, in certain scenarios. ScreenConnect host and guest cli

9.8 **CVE-2026-3207** Tibco bpm enterprise

Configuration issue in Java Management Extensions (JMX) in TIBCO BPM Enterprise version 4.x allows unauthorised access.

9.1 **CVE-2026-25534**

Impact Spinnaker updated URL Validation logic on user input to provide sanitation on user inputted URLs for clouddriver. However, they missed that Java URL objects do not correctly handle underscores on parsing. This led to a bypass of the previous CVE (CV

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. 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.