Daily brief, Tuesday, February 17, 2026

Feb 16, 7:00 PM to Feb 17, 7:00 PM ET

Generated Nov 7, 2026, 5:02 PM ET

0	4	0	8	0	1
Breaking	Newly exploited	Exploit code	Critical CVEs	Ransomware posts	New breaches

4 newly exploited, 8 new critical CVEs, 1 new breaches.

Breaking

Nothing spreading fast in technology large companies run.

Newly exploited in the wild

4

9.8 **CVE-2020-7796** Synacor Zimbra Collaboration Suite CISA KEV DETECTION

A server-side request forgery in Synacor Zimbra Collaboration Suite lets an attacker execute arbitrary system operations.

8.8 **CVE-2026-2441** Google Chromium CISA KEV

A remote attacker can corrupt the heap in Google Chromium CSS via a crafted HTML page, affecting Chromium-based browsers including Chrome and Edge.

8.8 **CVE-2008-0015** Microsoft Windows CISA KEV

The Windows Video ActiveX control in Microsoft Windows, with Windows Media Player installed, lets an attacker execute arbitrary code on the victim's system.

7.2 **CVE-2024-7694** TeamT5 ThreatSonar Anti-Ransomware CISA KEV

A remote attacker with administrator privileges can upload malicious files to TeamT5 ThreatSonar Anti-Ransomware because the product does not validate uploaded file content.

New public exploit code

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

New critical CVEs

8

9.8 **CVE-2020-7796** Synacor Zimbra Collaboration Suite KEV EXPLOIT CODE DETECTION

A server-side request forgery in Synacor Zimbra Collaboration Suite lets an attacker execute arbitrary system operations.

9.1 **CVE-2025-66614** Apache tomcat

Improper Input Validation vulnerability. This issue affects Apache Tomcat: from 11.0.0-M1 through 11.0.14, from 10.1.0-M1 through 10.1.49, from 9.0.0-M1 through 9.0.112. The following versions were EOL at the time the CVE was created but are known to be affect

9.9 **CVE-2025-59793** Rocketsoftware trufusion enterprise

Rocket TRUfusion Enterprise through 7.10.5 exposes the endpoint at /axis2/services/WsPortalV6UpDwAxis2Impl to authenticated users to be able to upload files. However, the application doesn't properly sanitize the jobDirectory parameter, which allows path trave

9.9 **CVE-2025-70830**

A Server-Side Template Injection (SSTI) vulnerability in the Freemarker template engine of Datart v1.0.0-rc.3 allows authenticated attackers to execute arbitrary code via injecting crafted Freemarker template syntax into the SQL script field.

9.6 **CVE-2026-22208**

OpenS100 (the reference implementation S-100 viewer) prior to commit 753cf29 contains a remote code execution vulnerability via an unrestricted Lua interpreter. The Portrayal Engine initializes Lua using luaL_openlibs() without sandboxing or capability restric

9.3 **CVE-2026-26220**

LightLLM version 1.1.0 and prior contain an unauthenticated remote code execution vulnerability in PD (prefill-decode) disaggregation mode. The PD master node exposes WebSocket endpoints that receive binary frames and pass the data directly to pickle.loads() w

9.8 **CVE-2026-1670**

The affected products are vulnerable to an unauthenticated API endpoint exposure, which may allow an attacker to remotely change the "forgot password" recovery email address.

9.8 **CVE-2026-23647**

Glory RBG-100 recycler systems using the ISPK-08 software component contain hard-coded operating system credentials that allow remote authentication to the underlying Linux system. Multiple local user accounts, including accounts with administrative privileges

Ransomware

No leak-site posts collected.

New data breaches 1

Canada Goose canadagoose.com 581,877 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.