Daily brief, Friday, February 20, 2026

Feb 19, 7:00 PM to Feb 20, 7:00 PM ET

Generated Nov 7, 2026, 4:34 PM ET

0	2	0	54	0	1
Breaking	Newly exploited	Exploit code	Critical CVEs	Ransomware posts	New breaches

2 newly exploited, 54 new critical CVEs, 1 new breaches.

Breaking

Nothing spreading fast in technology large companies run.

Newly exploited in the wild

2

9.9 **CVE-2025-49113** Roundcube Webmail CISA KEV DETECTION

Roundcube Webmail deserialization of untrusted data in upload.php lets an authenticated user achieve remote code execution via the _from URL parameter.

7.2 **CVE-2025-68461** Roundcube Webmail CISA KEV

Roundcube Webmail is vulnerable to cross-site scripting via an animate tag in an SVG document, letting an attacker run script in the victim's session.

New public exploit code

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

New critical CVEs

54

9.9 **CVE-2025-49113** Roundcube Webmail KEV EXPLOIT CODE DETECTION

Roundcube Webmail deserialization of untrusted data in upload.php lets an authenticated user achieve remote code execution via the _from URL parameter.

9.1 **CVE-2019-25444** Phpscriptsmall fiverr clone script

Fiverr Clone Script 1.2.2 contains an SQL injection vulnerability that allows unauthenticated attackers to manipulate database queries by injecting SQL code through the page parameter. Attackers can supply malicious SQL syntax in the page parameter to extract

9.4 **CVE-2026-26980** Ghost ghost DETECTION

Ghost is a Node.js content management system. Versions 3.24.0 through 6.19.0 allow unauthenticated attackers to perform arbitrary reads from the database. This issue has been fixed in version 6.19.1.

9.8 **CVE-2019-25441** Kostasmitroglou thesystem

thesystem 1.0 contains a command injection vulnerability that allows unauthenticated attackers to execute arbitrary system commands by submitting malicious input to the run_command endpoint. Attackers can send POST requests with shell commands in the command p

9.1 **CVE-2026-26988** Librenms librenms

LibreNMS is an auto-discovering PHP/MySQL/SNMP based network monitoring tool. Versions 25.12.0 and below contain an SQL Injection vulnerability in the ajax_table.php endpoint. The application fails to properly sanitize or parameterize user input when processin

9.5 **CVE-2026-21627**

The vulnerability was rooted in how the Tassos Framework plugin handled specific AJAX requests through Joomla's com_ajax entry point. Under certain conditions, internal framework functionality could be invoked without proper restriction.

9.8 **CVE-2026-26093** Owlcyberdefense opds-talon

+1 more CVEs in the same release

Improper Neutralization of Special Elements used in a Command ('Command Injection') in Owl opds 2.2.0.4 allows Command Injection via a crafted network request.

10.0 **CVE-2021-35402**

PROLiNK PRC2402M 20190909 before 2021-06-13 allows live_api.cgi?page=satellite_list OS command injection via shell metacharacters in the ip parameter (for satellite_status).

9.8 **CVE-2025-70831** Lkw199711 smanga

A Remote Code Execution (RCE) vulnerability was found in Smanga 3.2.7 in the /php/path/rescan.php interface. The application fails to properly sanitize user-supplied input in the mediaId parameter before using it in a system shell command. This allows an unaut

10.0 **CVE-2025-30411** Acronis cyber protect

+1 more CVEs in the same release

Sensitive data disclosure and manipulation due to improper authentication. The following products are affected: Acronis Cyber Protect 16 (Linux, Windows) before build 39938, Acronis Cyber Protect 15 (Linux, Windows) before build 41800.

9.8 **CVE-2026-2039** Gfi archiver

GFI Archiver MArc.Store Missing Authorization Authentication Bypass Vulnerability. This vulnerability allows remote attackers to bypass authentication on affected installations of GFI Archiver. Authentication is not required to exploit this vulnerability. The

9.8 **CVE-2026-2038** Gfi archiver

GFI Archiver MArc.Core Missing Authorization Authentication Bypass Vulnerability. This vulnerability allows remote attackers to bypass authentication on affected installations of GFI Archiver. Authentication is not required to exploit this vulnerability. The s

9.8 **CVE-2025-30410**

Sensitive data disclosure and manipulation due to missing authentication. The following products are affected: Acronis Cyber Protect Cloud Agent (Linux, macOS, Windows) before build 39870, Acronis Cyber Protect 16 (Linux, macOS, Windows) before build 39938, Ac

9.8 **CVE-2026-25715**
The web management interface of the device allows the administrator username and password to be set to blank values. Once applied, the device permits authentication with empty credentials over the web management interface and Telnet service. This effectively d

9.8 **CVE-2026-26974** Slyde.Js slyde
Slyde is a program that creates animated presentations from XML. In versions 0.0.4 and below, Node.js automatically imports **/*.plugin.{js,mjs} files including those from node_modules, so any malicious package with a .plugin.js file can execute arbitrary code

9.8 **CVE-2025-67995**
Deserialization of Untrusted Data vulnerability in LoftOcean PatioTime patiotime allows Object Injection.This issue affects PatioTime: from n/a through < 2.1.

9.8 **CVE-2026-27002** Openclaw openclaw
OpenClaw is a personal AI assistant. Prior to version 2026.2.15, a configuration injection issue in the Docker tool sandbox could allow dangerous Docker options (bind mounts, host networking, unconfined profiles) to be applied, enabling container escape or hos

9.3 **CVE-2026-25896** Naturalintelligence fast-xml-parser
fast-xml-parser allows users to validate XML, parse XML to JS object, or build XML from JS object without C/C++ based libraries and no callback. From 4.1.3to before 5.3.5, a dot (.) in a DOCTYPE entity name is treated as a regex wildcard during entity replacem

9.8 **CVE-2025-69371**
Deserialization of Untrusted Data vulnerability in AncoraThemes KindlyCare kindlycare allows Object Injection.This issue affects KindlyCare: from n/a through <= 1.6.1.

9.8 **CVE-2025-69372**
Deserialization of Untrusted Data vulnerability in AncoraThemes SevenHills sevenhills allows Object Injection.This issue affects SevenHills: from n/a through <= 1.6.2.

32 more critical CVEs in this window: see the dashboard

Ransomware

No leak-site posts collected.

New data breaches 1

CarMax carmax.com 431,371 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.