Daily brief, Thursday, March 19, 2026

Mar 18, 8:00 PM to Mar 19, 8:00 PM ET

Generated Nov 7, 2026, 11:40 AM ET

0	1	0	34	0	0
Breaking	Newly exploited	Exploit code	Critical CVEs	Ransomware posts	New breaches

1 newly exploited, 34 new critical CVEs.

Breaking

Nothing spreading fast in technology large companies run.

Newly exploited in the wild

1

10.0 **CVE-2026-20131** Cisco Secure Firewall Management Center (FMC) CISA KEV

Unauthenticated remote attacker executes arbitrary Java code via deserialization flaw in Cisco Secure Firewall Management Center (FMC) web interface.

New public exploit code

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

New critical CVEs

34

10.0 **CVE-2026-20131** Cisco Secure Firewall Management Center (FMC) KEV EXPLOIT CODE

Unauthenticated remote attacker executes arbitrary Java code via deserialization flaw in Cisco Secure Firewall Management Center (FMC) web interface.

10.0 **CVE-2026-32169** Microsoft azure cloud shell

Server-side request forgery (ssrf) in Azure Cloud Shell allows an unauthorized attacker to elevate privileges over a network.

9.9 **CVE-2026-26137** Microsoft 365 copilot chat

Server-side request forgery (ssrf) in Microsoft Exchange allows an authorized attacker to elevate privileges over a network.

9.1 **CVE-2026-22732** Vmware spring security

When applications specify HTTP response headers for servlet applications using Spring Security, there is the possibility that the HTTP Headers will not be written. This issue affects Spring Security Servlet applications using lazy (default) writing of HTTP Hea

10.0 **CVE-2026-22557** DETECTION

A malicious actor with access to the network could exploit a Path Traversal vulnerability found in the UniFi Network Application to access files on the underlying system that could be manipulated to access an underlying account.

9.0 **CVE-2026-27540**

Unrestricted Upload of File with Dangerous Type vulnerability in Rymera Web Co Pty Ltd. Woocommerce Wholesale Lead Capture allows Using Malicious Files. This issue affects Woocommerce Wholesale Lead Capture: through 2.0.3.1.

9.8 **CVE-2026-30872** Openwrt openwrt

+1 more CVEs in the same release

OpenWrt Project is a Linux operating system targeting embedded devices. In versions prior to 24.10.6 and 25.12.1, the mdns daemon has a Stack-based Buffer Overflow vulnerability in the match_ipv6_addresses function, triggered when processing PTR queries for IP

9.1 **CVE-2026-32238** Open-Emr openemr

OpenEMR is a free and open source electronic health records and medical practice management application. Versions prior to 8.0.0.2 contain a Command injection vulnerability in the backup functionality that can be exploited by authenticated attackers. The vulne

9.8 **CVE-2026-27542** DETECTION

Incorrect Privilege Assignment vulnerability in Rymera Web Co Pty Ltd. Woocommerce Wholesale Lead Capture allows Privilege Escalation. This issue affects Woocommerce Wholesale Lead Capture: through 2.0.3.1.

9.8 **CVE-2025-67113**

OS command injection in the CWMP client (/ftl/bin/cwmp) of Small Cell Sercomm SCE4255W (FreedomFi Englewood) firmware before DG3934v3@2308041842 allows remote attackers controlling the ACS endpoint to execute arbitrary commands as root via a crafted TR-069 Dow

9.8 **CVE-2026-32194** Microsoft bing images

Improper neutralization of special elements used in a command ('command injection') in Microsoft Bing Images allows an unauthorized attacker to execute code over a network.

9.0 **CVE-2026-32751** B3log siyuan

SiYuan is a personal knowledge management system. In versions 3.6.0 and below, the mobile file tree (MobileFiles.ts) renders notebook names via innerHTML without HTML escaping when processing renamenotebook WebSocket events. The desktop version (Files.ts) prop

9.8 **CVE-2026-32191** Microsoft bing images

Improper neutralization of special elements used in an os command ('os command injection') in Microsoft Bing Images allows an unauthorized attacker to execute code over a network.

9.8 **CVE-2026-30402** Wgstart wgcloud

An issue in wgcloud v.2.3.7 and before allows a remote attacker to execute arbitrary code via the test connection function

9.8 **CVE-2026-30694** Dedecms dedecms

An issue in DedeCMS v.5.7.118 and before allows a remote attacker to execute arbitrary code via the array_filter component

9.8 **CVE-2006-10003** Toddr xml\

XML::Parser versions through 2.47 for Perl has an off-by-one heap buffer overflow in st_serial_stack. In the case (stackptr == stacksize - 1), the stack will NOT be expanded. Then the new value will be written at location (++stackptr), which equals stacksize a

9.3 **CVE-2026-32754** Freescout freescout

FreeScout is a free help desk and shared inbox built with PHP's Laravel framework. Versions 1.8.208 and below are vulnerable to Stored Cross-Site Scripting (XSS) through FreeScout's email notification templates. Incoming email bodies are stored in the database

9.8 **CVE-2025-67114**

Use of a deterministic credential generation algorithm in /ftl/bin/calc_f2 in Small Cell Sercomm SCE4255W (FreedomFi Englewood) firmware before DG3934v3@2308041842 allows remote attackers to derive valid administrative/root credentials from the device's MAC ad

9.8 **CVE-2025-60237**

Deserialization of Untrusted Data vulnerability in Themeton Finag allows Object Injection.This issue affects Finag: from n/a through 1.5.0.

9.1 **CVE-2026-29103** Suitecrm suitecrm

SuiteCRM is an open-source, enterprise-ready Customer Relationship Management (CRM) software application. A Critical Remote Code Execution (RCE) vulnerability exists in SuiteCRM 7.15.0 and 8.9.2, allowing authenticated administrators to execute arbitrary syste

13 more critical CVEs in this window: see the dashboard

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.