Daily brief, Thursday, February 19, 2026

Feb 18, 7:00 PM to Feb 19, 7:00 PM ET

Generated Nov 7, 2026, 4:42 PM ET

0	0	0	26	0	0
Breaking	Newly exploited	Exploit code	Critical CVEs	Ransomware posts	New breaches

26 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

26

9.8 **CVE-2026-0926** DETECTION

The Prodigy Commerce plugin for WordPress is vulnerable to Local File Inclusion in all versions up to, and including, 3.3.0 via the 'parameters[template_name]' parameter. This makes it possible for unauthenticated attackers to include and read arbitrary files

9.8 **CVE-2025-71243** Spip saisies DETECTION

The 'Saisies pour formulaire' (Saisies) plugin for SPIP versions 5.4.0 through 5.11.0 contains a critical Remote Code Execution (RCE) vulnerability. An attacker can exploit this vulnerability to execute arbitrary code on the server. Users should immediately up

9.9 **CVE-2026-26030** Microsoft semantic kernel

Semantic Kernel, Microsoft's semantic kernel Python SDK, has a remote code execution vulnerability in versions prior to 1.39.4, specifically within the `InMemoryVectorStore` filter functionality. The problem has been fixed in version `python-1.39.4`. Users sho

9.8 **CVE-2026-1405** DETECTION

The Slider Future plugin for WordPress is vulnerable to arbitrary file uploads due to missing file type validation in the 'slider_future_handle_image_upload' function in all versions up to, and including, 1.0.5. This makes it possible for unauthenticated attac

9.8 **CVE-2026-27476**

RustFly 2.0.0 contains a command injection vulnerability in its remote UI control mechanism that accepts hex-encoded instructions over UDP port 5005 without proper sanitization. Attackers can send crafted hex-encoded payloads containing system commands to exec

9.8 **CVE-2026-2686**

A security vulnerability has been detected in SECCN Dingcheng G10 3.1.0.181203. This impacts the function qq of the file /cgi-bin/session_login.cgi. The manipulation of the argument User leads to os command injection. The attack is possible to be carried out r

9.1 **CVE-2025-13590** Wso2 api control plane

A malicious actor with administrative privileges can upload an arbitrary file to a user-controlled location within the deployment via a system REST API. Successful uploads may lead to remote code execution. By leveraging the vulnerability, a malicious actor ma

9.8 **CVE-2026-25242** Gogs gogs

Gogs is an open source self-hosted Git service. Versions 0.13.4 and below expose unauthenticated file upload endpoints by default. When the global RequireSigninView setting is disabled (default), any remote user can upload arbitrary files to the server via /re

9.8 **CVE-2026-26339** Hyland alfresco transform service

Hyland Alfresco Transformation Service allows unauthenticated attackers to achieve remote code execution through the argument injection vulnerability, which exists in the document processing functionality.

9.8 **CVE-2025-8350**

Execution After Redirect (EAR), Missing Authentication for Critical Function vulnerability in Inrove Software and Internet Services BiEticaret CMS allows Authentication Bypass, HTTP Response Splitting. This issue affects BiEticaret CMS: from 2.1.13 through 190

10.0 **CVE-2026-2731**

Path traversal and content injection in JobRunnerBackground.aspx in DynamicWeb 8 (all) and 9 (<9.19.7 and <9.20.3) allows unauthenticated attackers to execute code via simple web requests

9.8 **CVE-2025-67305** Commscope ruckus network director

In RUCKUS Network Director (RND) < 4.5.0.56, the OVA appliance contains hardcoded SSH keys for the postgres user. These keys are identical across all deployments, allowing an attacker with network access to authenticate via SSH without a password. Once authent

9.8 **CVE-2025-67304** Commscope ruckus network director

In Ruckus Network Director (RND) < 4.5.0.54, the OVA appliance contains hardcoded credentials for the ruckus PostgreSQL database user. In the default configuration, the PostgreSQL service is accessible over the network on TCP port 5432. An attacker can use the

10.0 **CVE-2025-15586**
OGP-Website installs prior git commit 52f865a4fba763594453068acf8fa9e3fc38d663 are affected by a type juggling flaw which if exploited can result in authentication bypass without knowledge of the victim account's password.

9.8 **CVE-2025-15559** Nestersoft worktime
An unauthenticated attacker can inject OS commands when calling a server API endpoint in NesterSoft WorkTime. The server API call to generate and download the WorkTime client from the WorkTime server is vulnerable in the “guid” parameter. This allows an attack

9.8 **CVE-2025-12882**
The Clasifico Listing plugin for WordPress is vulnerable to privilege escalation in versions up to, and including, 2.0. This is due to the plugin allowing users who are registering new accounts to set their own role by supplying the 'listing_user_role' paramet

9.8 **CVE-2026-23542**
Deserialization of Untrusted Data vulnerability in ThemeGoods Grand Restaurant grandrestaurant allows Object Injection.This issue affects Grand Restaurant: from n/a through <= 7.0.10.

9.8 **CVE-2026-23549**
Deserialization of Untrusted Data vulnerability in magepeopleteam WpEvently mage-eventpress allows Object Injection.This issue affects WpEvently: from n/a through <= 5.1.1.

9.8 **CVE-2026-1994**
The s2Member plugin for WordPress is vulnerable to privilege escalation via account takeover in all versions up to, and including, 260127. This is due to the plugin not properly validating a user's identity prior to updating their password. This makes it possi

9.1 **CVE-2025-55853** Softvision webpdf
SoftVision webPDF before 10.0.2 is vulnerable to Server-Side Request Forgery (SSRF). The PDF converter function does not check if internal or external resources are requested in the uploaded files and allows for protocols such as http:// and file:///. This all

6 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.