Daily brief, Wednesday, May 20, 2026

May 19, 8:00 PM to May 20, 8:00 PM ET

Generated Nov 7, 2026, 12:18 AM ET

0	7	0	22	0	0
Breaking	Newly exploited	Exploit code	Critical CVEs	Ransomware posts	New breaches

7 newly exploited, 22 new critical CVEs.

Breaking

Nothing spreading fast in technology large companies run.

Newly exploited in the wild

7

9.8 **CVE-2008-4250** Microsoft Windows CISA KEV

Remote attackers can execute arbitrary code on Microsoft Windows Server Service via a crafted RPC request that overflows a buffer during path canonicalization.

8.8 **CVE-2010-0806** Microsoft Internet Explorer CISA KEV

Remote attackers gain code execution in Microsoft Internet Explorer via a use-after-free that accesses an invalid pointer after object deletion.

8.8 **CVE-2010-0249** Microsoft Internet Explorer CISA KEV

A use-after-free flaw in Microsoft Internet Explorer lets remote attackers execute arbitrary code by accessing a pointer to a deleted object.

8.8 **CVE-2009-3459** Adobe Acrobat and Reader CISA KEV

Remote attackers can execute arbitrary code in Adobe Acrobat and Reader via a crafted PDF file that triggers a heap-based buffer overflow.

8.8 **CVE-2009-1537** Microsoft DirectX CISA KEV

Remote attackers execute arbitrary code via a crafted QuickTime media file triggering a NULL byte overwrite in Microsoft DirectX DirectShow.

7.8 **CVE-2026-41091** Microsoft Defender CISA KEV

An authorized local attacker can elevate privileges in Microsoft Defender by exploiting a link following flaw in how it handles file paths.

4.0 **CVE-2026-45498** Microsoft Defender CISA KEV

An unspecified flaw in Microsoft Defender allows an attacker to cause denial of service.

New public exploit code

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

New critical CVEs 22

9.8 **CVE-2008-4250** Microsoft Windows KEV EXPLOIT CODE
Remote attackers can execute arbitrary code on Microsoft Windows Server Service via a crafted RPC request that overflows a buffer during path canonicalization.

10.0 **CVE-2026-20223** Cisco secure workload
A vulnerability in the access validation of internal REST APIs of Cisco Secure Workload could allow an unauthenticated, remote attacker to access site resources with the privileges of the Site Admin role. This vulnerability is due to insufficient val

9.8 **CVE-2026-8631** Hp linux imaging and printing
A potential security vulnerability has been identified in the HP Linux Imaging and Printing Software. This potential vulnerability may allow escalation of privileges and/or arbitrary code execution via an integer overflow in the hpcups processing path when han

10.0 **CVE-2026-42960** Nlnetlabs unbound
NLnet Labs Unbound up to and including version 1.25.0 is vulnerable to poisoning via promiscuous records for the authority section. Promiscuous RRSets that complement DNS replies in the authority section can be used to trick Unbound to cache such records. If a

10.0 **CVE-2026-45444**
Unrestricted Upload of File with Dangerous Type vulnerability in WP Swings Gift Cards For WooCommerce Pro allows Using Malicious Files. This issue affects Gift Cards For WooCommerce Pro: from n/a through 4.2.6.

9.8 **CVE-2026-6555**
The ProSolution WP Client plugin for WordPress is vulnerable to Arbitrary File Upload in versions up to, and including, 2.0.0. This is due to an array validation mismatch where only the first file in the upload array undergoes extension and MIME type validatio

9.8 **CVE-2026-7284**
The Easy Elements for Elementor – Addons & Website Templates plugin for WordPress is vulnerable to privilege escalation via user registration in all versions up to, and including, 1.4.4. This is due to the 'easyel_handle_register' function not restricting what

9.8 **CVE-2026-24207** Nvidia triton inference server DETECTION
NVIDIA Triton Inference Server contains a vulnerability where an attacker could cause an authentication bypass. A successful exploit of this vulnerability might lead to code execution, escalation of privileges, data tampering, denial of service, or information

9.8 **CVE-2026-7637**

The Boost plugin for WordPress is vulnerable to PHP Object Injection in versions up to, and including, 2.0.3 via deserialization of untrusted input in the STYXKEY-BOOST_USER_LOCATION cookie. This makes it possible for unauthenticated attackers to inject a PHP

9.8 **CVE-2026-33278** Nlnetlabs unbound

NLnet Labs Unbound 1.19.1 up to and including version 1.25.0 has a vulnerability in the DNSSEC validator that enables denial of service and possible remote code execution as a result of deep copying a data structure and erroneously overwriting a destination po

9.8 **CVE-2026-9139**

Taiko AG1000-01A SMS Alert Gateway Rev 7.3 and Rev 8 contains a hard-coded credential vulnerability in the embedded web configuration interface where authentication is implemented entirely in client-side JavaScript in login.zhtml, exposing static plaintext cre

9.8 **CVE-2026-9141**

Taiko AG1000-01A SMS Alert Gateway Rev 7.3 and Rev 8 contains an authentication bypass vulnerability in the embedded web configuration interface that allows unauthenticated attackers to access internal application pages without any session management or server

9.5 **CVE-2026-8467**

Code Injection vulnerability in phenixdigital phoenix_storybook allows unauthenticated remote code execution via unsanitized attribute value interpolation in HEEx template generation. The psb-assign WebSocket event handler in 'Elixir.PhoenixStorybook.Story.Pla

9.4 **CVE-2026-39405**

Frappe Learning Management System (LMS) is a learning system that helps users structure their content. In versions 2.50.0 and below, a user with course editing role could upload a SCORM ZIP package to write files outside the intended directory. This issue has

9.4 **CVE-2026-9102**

A path traversal vulnerability exists in the Altium Enterprise Server ComparisonService due to missing filename sanitization in the Gerber file upload APIs. A regular authenticated workspace user can supply a crafted filename in the multipart Content-Dispositi

9.4 **CVE-2026-9129**

A path traversal vulnerability exists in the Altium Enterprise Server Viewer StorageController due to improper handling of file path route parameters. On on-premise deployments that use local filesystem storage, a regular authenticated user can supply a URL-en

9.3 **CVE-2026-9059**

NextGEN Gallery version prior to 4.2.1 are vulnerable to authenticated SQL injection via the 'orderby' parameter on the REST API endpoints '/imagely/v1/galleries' and '/imagely/v1/albums'. The root cause is an insufficient sanitization function ('_clean_column

9.3 **CVE-2026-9065**

SureCart version prior to 4.2.1 are vulnerable to authenticated SQL injection via multiple parameters ('model_name', 'model_id', 'integration_id', 'provider') on the REST API endpoint '/surecart/v1/integrations/{id}'. The root cause is a flawed escaping bypass

9.3 **CVE-2026-23734** DETECTION

XWiki Platform is a generic wiki platform. Versions prior to 18.1.0-rc-1, 17.10.3, 17.4.9, and 16.10.17 allow access to read configuration files by using URLs such as http://localhost:8080/bin/ssx/Main/WebHome?resource=/../../WEB-INF/xwiki.cfg&minify=false, le

9.3 **CVE-2026-33137**

XWiki Platform is a generic wiki platform offering runtime services for applications built on top of it. XWiki Platform is a generic wiki platform. In versions starting with 15.10.6 and prior to 18.1.0-rc-1, 17.10.3, 17.4.9, and 16.10.17, the POST /wikis/{wiki

2 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.