



[TLP: CLEAR]

Monthly Security Bulletin– August 2026

Overview

Greetings,
CERT Vanuatu (CERTVU), under the Department of Communication and Digital Transformation (DCDT), is pleased to share its **August 2026 Security Bulletin**. This edition provides an overview of significant vulnerabilities and emerging cyber threats identified during the month affecting commonly used systems and applications. The bulletin aims to support organizations in strengthening their **cybersecurity awareness, preparedness, and resilience** against evolving cyber threats.

Contacts

CERT Vanuatu (CERTVU)

<https://cert.gov.vu/>

Information

info@cert.gov.vu

Incident Reports

incident@cert.gov.vu

<https://cert.gov.vu/index.php/services/incident-resolution>

Threat Intelligence

Vulnerabilities and exploits

Unauthenticated PHP Object Injection To Remote Code Execution On GiveWP

"This blog post is about an unauthenticated remote code execution vulnerability in the GiveWP plugin. An attacker with no account can run arbitrary commands on the server of a GiveWP site that has one published donation form and one active payment gateway which, on the versions where the chain is fully reachable, describes a default installation. The flaw chains a broken "safe unserialize" helper, a donation flow that feeds that helper attacker-controlled data, and a gadget chain in code that GiveWP ships. Patchstack has issued mitigation rules to protect against exploitation of this vulnerability."

CERTVU recommends all users and organizations to read this advisory and follow the mitigation steps to mitigate these vulnerabilities.

<https://patchstack.com/articles/unauthenticated-php-object-injection-to-remote-code-execution-on-givewp/>

ServiceNow Warns Of Three Max Severity Security Vulnerabilities

"ServiceNow released security patches for three new maximum-severity AI Platform vulnerabilities that can be exploited in code injection, SQL injection, and privilege escalation attacks. The ServiceNow AI Platform (formerly known as the Now Platform) is an enterprise-grade Platform-as-a-Service (PaaS) that 1/9 helps integrate AI into core enterprise workflows and powers more than 100,000 enterprise AI apps at 85% of all Fortune 500 companies. In a Thursday advisory, the company said it patched its cloud-based platform against the three critical security flaws (CVE-2026-18885, CVE-2026-18886, and CVE-2026-74820) and advised customers to secure their self-hosted instances." CERTVU recommends all users and organizations to read this vulnerability and follow the mitigation steps to mitigate these vulnerabilities.

<https://www.bleepingcomputer.com/news/security/servicenow->

[warns-of-three-max-severity-security-vulnerabilities/](https://patchstack.com/articles/unauthenticated-php-object-injection-to-remote-code-execution-on-givewp/)

Unauthenticated PHP Object Injection To Remote Code Execution On GiveWP

"This blog post is about an unauthenticated remote code execution vulnerability in the GiveWP plugin. An attacker with no account can run arbitrary commands on the server of a GiveWP site that has one published donation form and one active payment gateway which, on the versions where the chain is fully reachable, describes a default installation. The flaw chains a broken "safe unserialize" helper, a donation flow that feeds that helper attacker-controlled data, and a gadget chain in code that GiveWP ships. Patchstack has issued mitigation rules to protect against exploitation of this vulnerability."

CERTVU recommends all users and organizations to read this advisory and follow the mitigation steps to mitigate these vulnerabilities.

<https://patchstack.com/articles/unauthenticated-php-object-injection-to-remote-code-execution-on-givewp/>

ServiceNow Warns Of Three Max Severity Security Vulnerabilities

"ServiceNow released security patches for three new maximum-

severity AI Platform vulnerabilities that can be exploited in code injection, SQL injection, and privilege escalation attacks. The ServiceNow AI Platform (formerly known as the Now Platform) is an enterprise-grade Platform-as-a-Service (PaaS) that helps integrate AI into core enterprise workflows and powers more than 100,000 enterprise AI apps at 85% of all Fortune 500 companies. In a Thursday advisory, the company said it patched its cloud-based platform against the three critical security flaws (CVE-2026-18885, CVE-2026-18886, and CVE-2026-74820) and advised customers to secure their self-hosted instances." CERTVU recommends all users and organizations to read this advisory and follow the mitigation steps to mitigate these vulnerabilities.

<https://www.bleepingcomputer.com/news/security/servicenow-warns-of-three-max-severity-security-vulnerabilities/>

One Slug, Seven Editions: The MiniOrange SAML SSO Bug That Let Anyone Log In As Your WordPress Admin

"Most vulnerability write-ups are about the bug. This is primarily about everything around the bug, where the actual risk ended up living. The DigitalOcean security team identified a critical gap the hard way, based on their defense-in-depth controls. The version-level

analysis that follows, which no public vulnerability database had, came out of DigitalOcean's work. Two critical authentication bypasses (CVSS 9.8) were publicly disclosed in July 2026 for the miniOrange SAML 2.0 Single Sign On plugin (opens in new tab). Both allow an unauthenticated attacker to forge a SAML assertion and land in /wp admin as any existing user, including administrators."

CERTVU recommends all users and organizations to read this Vulnerability and follow the mitigation steps to mitigate these vulnerabilities.

<https://patchstack.com/articles/one-slug-seven-editions-the-miniorange-saml-sso-bug-that-let-anyone-log-in-as-yourwordpress-admin/>

Microsoft Warns Of Max Severity Entra ID Flaw Exploited In Attacks

"Microsoft has patched a maximum-severity vulnerability in the Entra ID identity and access management (IAM) platform that has been exploited in attacks. Formerly known as Azure Active Directory (or Azure AD), it is a cloud-based IAM platform that provides Microsoft 365, Azure, or Dynamics CRM Online customers with authentication, policy enforcement, and protection across apps and resources. Tracked as CVE-2026-69836, this critical security

flaw was discovered by Microsoft principal security engineer Robert Fitzpatrick, and it allowed threat actors with no privileges to gain code execution in low-complexity attacks."

CERTVU recommends all users and organizations to read this Vulnerability and follow the mitigation steps to mitigate these vulnerabilities.

<https://www.bleepingcomputer.com/news/microsoft/microsoft-warns-of-max-severity-entra-id-flaw-exploited-in-attacks/>

Cisco Patches Nine Crosswork And Secure Workload Flaws, Five Scoring CVSS 10.0

"Cisco has published another round of security updates for Crosswork platforms and Secure Workload Software as part of a continued comprehensive internal security review. Four of the security vulnerabilities affect Crosswork Data Gateway, Crosswork Network Controller, and Crosswork Planning, regardless of the device configuration. A brief description of each of the flaws is below -"

CERTVU recommends all users and organizations to read this Vulnerability and follow the mitigation steps to mitigate these vulnerabilities.

<https://thehackernews.com/2026/08/cisco-patches-nine-crosswork-and-secure.html>

Cisco Patches Critical Crosswork, Secure Workload Vulnerabilities

"Cisco on Wednesday announced patches for 15 vulnerabilities across its products, including critical and high-severity flaws in Crosswork and Secure Workload. Crosswork version 7.2.1-SP was released with fixes for four critical-severity CVEs. Three of them, CVE-2026-20030, CVE-2026-20357, and CVE 2026-20358, have a maximum severity rating (CVSS score of 10/10), while the fourth, CVE-2026-20359, has a near-max severity (CVSS score of 9.9/10)."

CERTVU recommends all users and organizations to read this Vulnerability and follow the mitigation steps to mitigate these vulnerabilities.

<https://www.securityweek.com/cisco-patches-critical-crosswork-secure-workload-vulnerabilities/>

943 Patches Rolled Out With Oracle's August 2026 Security Update

"Oracle on Tuesday announced the release of 943 new security patches as part of the August 2026 Critical Security Patch Update (CSPU), its third monthly security rollout. The company's advisory mentions more than 1,000 unique CVEs across two dozen products, including over 460

vulnerabilities that can be exploited remotely without authentication. The patches for dozens of vulnerabilities address additional security flaws. More than 150 of the security defects are critical-severity bugs, and nearly 90 of them have a CVSS score of 9.8 or higher."

CERTVU recommends all users and organizations to read this Vulnerability and follow the mitigation steps to mitigate these vulnerabilities.

<https://www.securityweek.com/943-patches-rolled-out-with-oracles-august-2026-security-update/>

40,000 WordPress Sites Affected By Authentication Bypass Vulnerability In User Profile Builder WordPress Plugin

"On July 14th, 2026, we received a submission for an Authentication Bypass vulnerability in User Profile Builder, a WordPress plugin with more than 40,000 active installations. This vulnerability makes it possible for unauthenticated attackers to log in as the user with ID 1, which is typically the site administrator, resulting in full administrative takeover of the site. The vulnerability is only exploitable on sites where the plugin's Automatically Log In setting is enabled. Props to Supakiad S. (m3ez) who discovered and responsibly reported this

vulnerability through the Wordfence Bug Bounty Program. This researcher earned a bounty of \$975.00 for this discovery."

CERTVU recommends all users and organizations to read this Vulnerability and follow the mitigation steps to mitigate these vulnerabilities.

<https://www.wordfence.com/blog/2026/08/40000-wordpress-sites-affected-by-authentication-bypass-vulnerability-in-userprofile-builder-wordpress-plugin/>

600,000 WordPress Sites Affected By Arbitrary File Upload Vulnerability In Forminator Forms WordPress Plugin

"On July 14th, 2026, we received a submission for an Unauthenticated Arbitrary File Upload vulnerability in Forminator Forms, a WordPress plugin with more than 600,000 active installations. This vulnerability makes it possible for unauthenticated attackers to upload arbitrary files, including executable PHP files, to a vulnerable site, which can lead to remote code execution and complete site compromise. The vulnerability is only exploitable on sites that have a form containing both a File Upload field and a Select field."

CERTVU recommends all users and organizations to read this Vulnerability and follow the

mitigation steps to mitigate these vulnerabilities.

<https://www.wordfence.com/blog/2026/08/600000-wordpress-sites-affected-by-arbitrary-file-upload-vulnerability-informator-forms-wordpress-plugin/>

Adobe Urges Immediate Patching Of Critical ColdFusion, Campaign Classic Flaws

"Adobe on Tuesday rolled out patches for over 50 vulnerabilities across its products, including critical severity bugs in ColdFusion, Campaign Classic, and Commerce. With a priority 1 rating, the ColdFusion update fixes 15 security defects, including three flagged as critical that could lead to arbitrary code execution and application denial-of-service (DoS). These include an OS command injection tracked as CVE-2026-48362 (CVSS score of 10/10), an eval injection tracked as CVE-2026-48273 (CVSS score of 9.9/10), and an incorrect authorization tracked as CVE-2026-71384 (CVSS score of 9.6/10)."

CERTVU recommends all users and organizations to read this Vulnerability and follow the mitigation steps to mitigate these vulnerabilities.

<https://www.securityweek.com/adobe-urges-immediate-patching-of-critical-coldfusion-campaign-classic-flaws/>

SAP Patches Critical Code Injection, Memory Corruption Vulnerabilities

"Enterprise software maker SAP on Tuesday announced the release of 28 new security notes, two updates to previous notes, and a GitHub advisory. Four of the notes published on SAP's August 2026 Security Patch Day resolve critical vulnerabilities, the most severe of which is CVE-2026-58231 (CVSS score of 10/10), an improper authorization issue in SAP Commerce Cloud (Data Hub Adapter). The bug 2/11 could allow remote attackers to bypass authentication, likely leading to code execution and unauthorized access to internal components. Successful exploitation would impact the confidentiality, integrity, and availability of the application." CERTVU recommends all users and organizations to read this Vulnerability and follow the mitigation steps to mitigate these vulnerabilities.

<https://www.securityweek.com/sap-patches-critical-code-injection-memory-corruption-vulnerabilities/>

Metabase SQLi Zero-Day Exploited In Customer Data-Theft Attacks

"A critical Metabase SQL injection vulnerability was exploited in zero-day attacks to breach customer instances in data theft attacks,

known to impact Framework and Tally. Metabase disclosed the attacks on Thursday, warning that its Metabase Cloud SaaS platform was compromised through a previously unknown vulnerability affecting versions 1.58 and above. The company warns that self-hosted installations are also vulnerable. "We recently identified that Metabase Cloud was attacked by someone utilizing an unknown ("0-day") security vulnerability in versions 1.58 and above," Metabase CEO Sameer Al-Sakran warned in a blog post."

CERTVU recommends all users and organizations to read this Vulnerability and follow the mitigation steps to mitigate these vulnerabilities.

<https://www.bleepingcomputer.com/news/security/framework-tally-disclose-metabase-data-theft-attacks/>

Malware

Active Exploitation Of CVE-2026–59310: 361 Victim IPs Across 47 Countries

"QUIRSO's Threat Research team is tracking an active exploitation campaign targeting internet accessible VMware vCenter systems. Based on evidence collected during a recent incident response engagement, we assess that a suspected advanced persistent threat (APT) actor is exploiting CVE 2026–59310 and

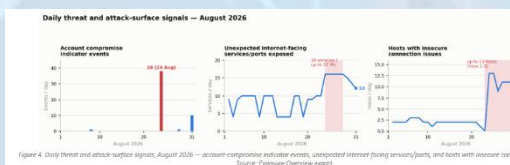
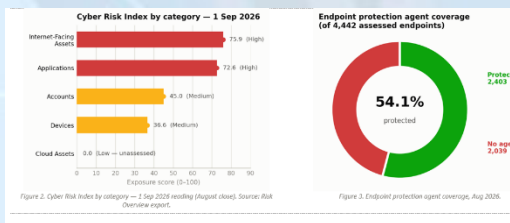
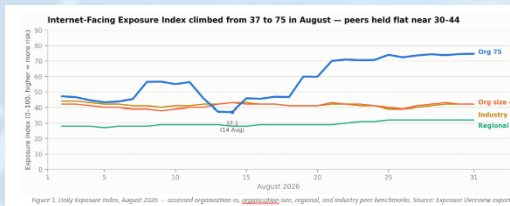
using reverse SSH to maintain access to compromised systems. CVE-2026–59310 is a critical directory-traversal vulnerability in the VMware vCenter Syslog server. According to Broadcom, an attacker with network access to vCenter may exploit the vulnerability to execute arbitrary code."

https://medium.com/@quirso_de/active-exploitation-of-cve-2026-59310-361-victim-ips-across-47-countries-9783187cc6ff

CERTVU Threat Statistics

This bulletin condenses a monthly Cybersecurity Report — TrendAI Vision One™ exposure, configuration, and MDR data, refreshed against the 1 Sep Risk Overview — into a compact, anonymized summary. The reporting organization's identity, department names, and other identifying details have been generalized or removed prior to distribution. The composite **Cyber Risk Index closed August at 64.9/100 ("Medium")**, roughly double every peer benchmark (34–38). The clearest warning sign is a near-doubling of the **internet-facing Exposure Index, from 37 to 75 (75.9 by 1 Sep)**, still High risk as medium-risk public IPs nearly double. No incidents were confirmed, but two MDR cases remain open and the coverage and

patch-cadence gaps behind this risk are unchanged.



Key Findings

- Endpoint coverage: 45.9% of endpoints (2,039) have no protection agent; 43.4% have no telemetry sensor.
- Patch backlog: MTTP ~100 days vs. 8–10 global; 97.5–98.5% of devices carry ≥1 detected vulnerability.
- Active exploitation: 375 actively-exploited CVEs, 89% still unaddressed by status.
- Hardening gaps: Firewall & Application Control disabled on 100% of standard endpoints.
- Email spoofing risk: Outbound DKIM 0%, SPF/DMARC ~24% complete across 17 domains.

- MDR: 2 “Noteworthy” cases open (a single internal department); 0 confirmed incidents; MTTA up 22%.
- Threat spike: Account-compromise indicators jumped to 38 events on 24 Aug (vs. 0–1 baseline), one day before an MDR case opened.
- Post month-end (1 Sep): Internet-Facing Assets exposure rose further to 75.9 (High); medium-risk public IPs nearly doubled to 23 (from 12) and discovered devices grew to 8,856.

Priority Recommendations

- Critical — Close the endpoint agent/sensor coverage gap, prioritising internet-facing assets and the affected department's systems.
- Critical — Work the 144-CVE critical shortlist and 375 actively-exploited CVEs; target a material MTTP reduction.
- Critical — Drive both open MDR cases to a documented root cause and closure.
- High — Enable Firewall and Application Control across Standard Endpoint Protection.
- High — Complete outbound SPF/DKIM/DMARC across all 17 registered domains.

CERTVU Advisories

Advisory 284: D-Link DIR-825M LTE Firmware Upgrade Stack-Based Buffer Overflow (CVE-2026-82593)

CVE-2026-82593 is a stack-based buffer overflow in the LTE Module Firmware Upgrade component of the D-Link DIR-825M, a mass-market wireless router with an LTE fallback/upgrade path, sold through general electronics retailers, with no dependency on a specific fixed-line ISP.

CERTVU notes that no new international alert on BADBOX 2.0 has been issued since the FBI Public Service Announcement, which remains the current standing warning. Despite the threat having been publicly known for more than a year, infected devices remain active in Vanuatu.

<https://cert.gov.vu/index.php/advisories/302-advisory-284>

Advisory 283: D-Link DNS-3xxL NAS Series Multiple OS Command Injection Vulnerabilities (CVE-2026-82689, CVE-2026-82692, and CVE-2026-85223)

CVE-2026-82689, CVE-2026-82692, and CVE-2026-85223 are three OS command injection vulnerabilities in the web-management CGI scripts of D-Link's DNS-3xxL ShareCenter NAS series, a mass-market consumer/small-office storage line sold through general electronics retailers worldwide. CVE-2026-82689 affects /cgi-bin/isomount_mgr.cgi (the "upIsoRootPath" parameter) on DNS-320L, DNS-327L, DNS-340L,

and DNS-345; CVE-2026-82692 affects /cgi-bin/iscsi_mgr.cgi (the "alias"/"username"/"password"/"volume_location" parameters) on DNS-340L and DNS-345; and CVE-2026-85223 affects /cgi-bin/dropbox.cgi (the "callback_url"/"sync_interval" parameters) on DNS-340L specifically. All three allow a remote, low-privileged attacker to inject and execute arbitrary operating system commands.

<https://cert.gov.vu/index.php/advisories/301-advisory-283>

Advisory 282: Tenda AC18 Telnet Handler Missing Authentication Vulnerability (CVE-2026-82695)

CVE-2026-82695 is a missing-authentication vulnerability in the Telnet Handler component of the Tenda AC18, a mass-market AC1900-class dual-band Wi-Fi router sold through general electronics retailers worldwide (Amazon, eBay, and other consumer retail channels), with no dependency on any specific ISP.

<https://cert.gov.vu/index.php/advisories/300-advisory-282>

Advisory 281: Tenda AC1206 Web UI Missing Authentication Vulnerabilities (CVE-2026-82693 and CVE-2026-82694)

CVE-2026-82693 and CVE-2026-82694 are two missing-

authentication vulnerabilities in the Web UI of the Tenda AC1206, a mass-market AC1900-class dual-band Wi-Fi router sold through general electronics retailers worldwide (Amazon, eBay, and other consumer retail channels), with no dependency on any specific ISP.

<https://cert.gov.vu/index.php/advisories/299-advisory-281>

Advisory 280: TOTOLINK NR1800X setUploadSetting Stack-Based Buffer Overflow (CVE-2026-82616)

CVE-2026-82616 is a critical stack-based buffer overflow in the setUploadSetting function of the file /cgi-bin/cstecgi.cgi on the TOTOLINK NR1800X, a mass-market, SIM-card-based 5G/LTE Wi-Fi 6 router sold through general electronics retailers internationally (including Amazon and multiple European and African online retailers), with no dependency on a specific local ISP or fixed-line service – any individual with a compatible mobile SIM can purchase and deploy one.

<https://cert.gov.vu/index.php/advisories/298-advisory-280>

Advisory 278: Dell PowerStore Management Interface Missing Authentication for Critical Function Vulnerability (CVE-2026-58574)

CVE-2026-58574 (CVSS 3.1 base score 9.8, Critical, CWE-306: Missing Authentication for Critical Function) affects the management interface of Dell PowerStore. An unauthenticated remote attacker with network access to the restricted management interface can exploit the vulnerability to read internal system information directly from the appliance filesystem, with no privileges or user interaction required, potentially exposing credentials that grant full administrative access to the array.

<https://cert.gov.vu/index.php/advisories/296-advisory-278>

Events

Cyber Month Activities

October is observed as **Cyber Month in Vanuatu**, dedicated to promoting the safe and responsible use of digital technology and strengthening public awareness of cybersecurity.

As part of the **Cyber Up Pacific** campaign, CERT Vanuatu (CERTVU) coordinates Cyber Week awareness activities targeting schools, communities, government agencies, businesses, and other stakeholders. These initiatives aim to educate the public about emerging cyber threats, promote secure online practices, and encourage individuals and organizations to take proactive

measures to safeguard their information and digital systems. Through these activities, CERTVU contributes to building a **safer, more secure, and resilient digital environment for Vanuatu.**

CERT Vanuatu Initiatives

Strengthening National Cybersecurity

CERT Vanuatu (CERTVU) works alongside national, regional, and international partners to improve cybersecurity awareness, enhance technical capabilities, and strengthen the country's ability to prevent and respond to cyber threats.

Cybersecurity Awareness and Outreach

CERTVU promotes cybersecurity knowledge through radio programs, social media platforms, public awareness campaigns, and the distribution of educational materials to encourage safer digital practices among the public.

National Cybersecurity Development

The Department of Communication and Digital Transformation (DCDT) is progressing the development of a **Cloud Infrastructure Roadmap** and the establishment of a **Cybersecurity Agency**. These initiatives aim to support secure digital transformation, improve

cybersecurity governance, and strengthen coordination at the national level.

Capacity Building and Skills Development

CERTVU supports cybersecurity training and knowledge-sharing activities to strengthen the skills of government agencies and critical infrastructure organizations in identifying, preventing, and managing cyber risks.

Regional and International Cooperation

CERTVU engages in regional cybersecurity initiatives, including the **Pacific Cyber Security Operational Network (PaCSO)**, to promote collaboration, exchange threat information, share expertise, and support cybersecurity capacity development across the Pacific.

Cyber Incident Response

CERTVU monitors, analyses, and responds to reported cyber incidents, providing guidance and technical assistance to affected organizations. These efforts help strengthen incident management, minimize potential impacts, and support recovery from cyber threats.

References

1. <https://www.bleepingcomputer.com/news/security/framework-tally-disclose-metabase-data-theft-attacks/>
2. <https://thehackernews.com/2026/08/metabase-zero-day-exploited-in-wild.html>
3. <https://securityaffairs.com/196874/hacking/metabase-zero-day-exploited-in-the-wild-exposing-admin-access-and-sensitivedata.html>
4. <https://www.securityweek.com/sap-patches-critical-code-injection-memory-corruption-vulnerabilities/>
5. <https://www.securityweek.com/adobe-urges-immediate-patching-of-critical-coldfusion-campaign-classic-flaws/>
7. <https://www.wordfence.com/blog/2026/08/40000-wordpress-sites-affected-by-authentication-bypass-vulnerability-in-userprofile-builder-wordpress-plugin/>
8. <https://www.infosecurity-magazine.com/news/wordpress-plugin-flaw-40000-sites/>
9. <https://thehackernews.com/2026/08/forminator-wordpress-flaw-can-enable.html>
10. <https://www.wordfence.com/blog/2026/08/600000-wordpress-sites-affected-by-arbitrary-file-upload-vulnerability-informinator-forms-wordpress-plugin/>
11. <https://www.bleepingcomputer.com/news/security/sap-warns-of-critical-flaws-in-netweaver-and-commerce-cloud/>
12. <https://www.securityweek.com/943-patches-rolled-out-with-oracles-august-2026-security-update/>
13. <https://www.securityweek.com/cisco-patches-critical-crosswork-secure-workload-vulnerabilities/>
14. <https://www.bleepingcomputer.com/news/microsoft/microsoft-warns-of-max-severity-entra-id-flaw-exploited-in-attacks/>
15. <https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-69836>
16. <https://thehackernews.com/2026/08/microsoft-entra-id-flaw-cvss-100.html>
17. <https://www.securityweek.com/microsoft-rolls-out-22-fresh-security-patches/>
18. <https://www.helpnetsecurity.com/2026/08/21/microsoft-entra-id-vulnerability-cve-2026-69836/>
19. <https://thehackernews.com/2026/08/cisco-patches-nine-crosswork-and-secure.html>
20. <https://securityaffairs.com/197640/security/six-maximum-severity-flaws-found-in-cisco-products.html>
21. <https://www.theregister.com/security/2026/08/21/cisco-bug-severity-warning-reads-like-olympic-gymnastics-scores-10-1099-96-and-75/5290838>
22. <https://patchstack.com/articles/one-slug-seven-editions-the-miniorange-saml-ss0-bug-that-let-anyone-log-in-as-your-wordpress-admin/>
23. <https://www.bleepingcomputer.com/news/security/hackers-target-wordpress-sites-in-miniorange-auth-bypass-attacks/>
24. <https://patchstack.com/articles/unauthenticated-php-object-injection-to-remote-code-execution-on-givewp/>

25. <https://www.bleepingcomputer.com/news/security/givewp-wordpress-donation-plugin-flaw-lets-hackers-execute-servercommands/>
26. <https://thehackernews.com/2026/08/five-critical-wordpress-plugin-and.html>
27. <https://www.bleepingcomputer.com/news/security/servicenow-warns-of-three-max-severity-security-vulnerabilities/>
28. <https://thehackernews.com/2026/08/three-cvss-100-servicenow-flaws-could.html>
29. <https://patchstack.com/articles/unauthenticated-php-object-injection-to-remote-code-execution-on-givewp/>
30. <https://www.bleepingcomputer.com/news/security/givewp-wordpress-donation-plugin-flaw-lets-hackers-execute-servercommands/>
31. <https://thehackernews.com/2026/08/five-critical-wordpress-plugin-and.html>
32. <https://www.bleepingcomputer.com/news/security/servicenow-warns-of-three-max-severity-security-vulnerabilities/>
33. <https://thehackernews.com/2026/08/three-cvss-100-servicenow-flaws-could.html>
34. https://medium.com/@quirso_de/active-exploitation-of-cve-2026-59310-361-victim-ips-across-47-countries-9783187cc6ff
35. <https://thehackernews.com/2026/08/attackers-exploit-vmware-vcenter.html>
36. <https://cert.gov.vu/index.php/advisories>
37. <https://www.facebook.com/CERTVU>