[TLP: CLEAR]

Monthly Security Bulletin– January 2026

Overview

Greetings,

CERT Vanuatu, an operational unit of the Office of the Department of Communication and Digital Transformation, is pleased to present this Monthly Security Bulletin. This edition highlights key vulnerabilities and active exploits identified throughout January 2026 across widely used systems and applications. The bulletin is intended to serve as a valuable resource to support and strengthen your organization's cybersecurity preparedness.

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

Adobe Patches Critical Apache Tika Bug In ColdFusion

"Adobe has released security updates for 11 products on January 2026 Patch Tuesday, addressing a total of 25 vulnerabilities, including a critical code execution flaw. The critical-severity issue, tracked as CVE-2025-66516 (CVSS score of 10/10), is an XML External Entity (XXE) injection bug in Apache Tika modules that could be exploited via XFA files placed inside PDF documents. The security defect was patched in early December, when Apache warned that successful exploitation could lead to information

leaks, SSRF attacks, denial-of-service (DoS), or remote code execution (RCE)."
CERTVU recommends all users and organizations to read this vulnerability and follow the mitigation steps to mitigate these vulnerabilities.

https://www.securityweek.com/adobe-patches-critical-apache-tika-bug-in-coldfusion/

Critical Privilege Escalation Vulnerability In Modular DS Plugin Affecting
40k+ Sites Exploited In The Wild

"This blog post is about an Unauthenticated Privilege Escalation vulnerability in the Modular DS plugin.
Patchstack has issued a mitigation rule to protect against exploitation of this vulnerability. If you're a Modular DS user, please update to at least version 2.5.2. This vulnerability was discovered and reported to Patchstack by Teemu Saarentaus from group.one."
CERTVU recommends all users and organizations to read this vulrability and follow the mitigation steps to mitigate these vulnerabilities.

https://thehackernews.com/2026/01/critical-wordpress-modular-ds-plugin.html

Cisco Finally Fixes Max-Severity Bug Under Active Attack For Weeks

"Cisco finally delivered a fix for a maximum-severity bug in AsyncOS that has been under attack for at least a month. The networking giant disclosed the vulnerability, tracked as CVE-2025-20393, on December 17. It affects some Secure Email Gateway (SEG) and Secure Email and Web Manager (SEWM) appliances. Cisco first became aware of attackers targeting the appliances on December 10."
CERTVU recommends all users and organizations to read this advisory and follow the mitigation steps to mitigate these vulnerabilities.

https://www.theregister.com/2026/01/15/cisco_fixes_cve_2025_20393/

Patch Now: Active Exploitation Underway For Critical HPE OneView Vulnerability

"Check Point Research has identified an active, coordinated exploitation campaign targeting CVE-202537164, a critical remote code execution vulnerability affecting HPE OneView. The activity, observed directly in Check Point telemetry, is attributed to the RondoDox botnet and represents a sharp escalation from early probing attempts to large-scale, automated attacks. Check Point has already

blocked tens of thousands of exploitation attempts, underscoring both the severity of the vulnerability and the urgency for organizations to act. On January 7, 2026 Check Point Research reported the campaign to CISA, and the vulnerability was added to the Known Exploited Vulnerabilities KEV catalog the same day."
CERTVU recommends all users and organizations to read this advisory and follow the mitigation steps to mitigate these vulnerabilities.

https://blog.checkpoint.com/research/patch-now-active-exploitation-underway-for-critical-hpe-oneview-vulnerability/

100,000 WordPress Sites Affected By Privilege Escalation Vulnerability In Advanced Custom Fields: Extended WordPress Plugin
"On December 10th, 2025, we received a submission for a Privilege Escalation vulnerability in Advanced Custom Fields: Extended, a WordPress plugin with more than 100,000+ active installations. This vulnerability makes it possible for an unauthenticated attacker to grant themselves administrative privileges by updating the user role on a user action form where a role can be selected. Props to andrea bocchetti who discovered and responsibly reported this vulnerability through the Wordfence Bug Bounty Program."
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/acf-plugin-bug-gives-hackers-admin-on-50-000-wordpress-sites/

Zoom And GitLab Release Security Updates Fixing RCE, DoS, And 2FA Bypass Flaws
"Zoom and GitLab have released security updates to resolve a number of security vulnerabilities that could result in denial-of-service (DoS) and remote code execution. The most severe of the lot is a critical security flaw impacting Zoom Node Multimedia Routers (MMRs) that could permit a meeting participant to conduct remote code execution attacks. The vulnerability, tracked as CVE-2026-22844 and discovered internally by its Offensive Security team, carries a CVSS score of 9.9 out of 10.0."
CERTVU recommends all users and organizations to read this Vulnerability and follow the mitigation steps to mitigate these vulnerabilities.

https://thehackernews.com/2026/01/zoom-and-gitlab-release-security.html

Oracle's First 2026 CPU Delivers 337 New Security Patches

"Oracle has released 337 new security patches for over 30 products as part of its first Critical Patch Update (CPU) for 2026. There appear to be roughly 230 unique CVEs in Oracle's January 2026 CPU advisory. More than two dozen of the fresh fixes resolve critical-severity vulnerabilities and over 235 patches address flaws that are remotely exploitable without authentication. Roughly half a dozen patches address CVE-2025-66516 (CVSS score of 10/10), a critical defect in Apache Tika that could lead to XML External Entity (XXE) injection attacks."
CERTVU recommends all users and organizations to read this Vulnerability and follow the mitigation steps to mitigate these vulnerabilities.

https://www.securityweek.com/oracles-first-2026-cpu-delivers-337-new-security-patches/

Critical Arbitrary File Upload Vulnerability In RealHomes CRM Plugin affecting 30k+ Sites
"This blog post is about a Subscriber+ arbitrary file upload vulnerability in the RealHomes CRM. If you're a RealHomes CRM user, please update to at least version 1.0.1."
CERTVU recommends all users and organizations to read this Vulnerability and follow the mitigation steps to mitigate these vulnerabilities.

https://patchstack.com/articles/critical-arbitrary-file-upload-vulnerability-in-realhomes-crm-plugin-affecting-30k-sites/

Critical GNU InetUtils Telnetd Flaw Lets Attackers Bypass Login And Gain Root Access
"A critical security flaw has been disclosed in the GNU InetUtils telnet daemon (telnetd) that went unnoticed for nearly 11 years. The vulnerability, tracked as CVE-2026-24061, is rated 9.8 out of 10.0 on the CVSS scoring system. It affects all versions of GNU InetUtils from version 1.9.3 up to and including version 2.7. "Telnetd in GNU Inetutils through 2.7 allows remote authentication bypass via a '-f root' value for the USER environment variable," according to a description of the flaw in the NIST National Vulnerability Database (NVD)."
CERTVU recommends all users and organizations to read this Vulnerability and follow the mitigation steps to mitigate these vulnerabilities.

https://thehackernews.com/2026/01/critical-gnu-inetutils-telnetd-flaw.html

Critical Sandbox Escape Flaw Found In Popular Vm2 NodeJS Library
"A critical-severity vulnerability in the vm2 Node.js sandbox library, tracked as CVE-2026-22709, allows

escaping the sandbox and executing arbitrary code on the underlying host system. The open-source
vm2 library creates a secure context to allow users to execute untrusted JavaScript code that does not
have access to the filesystem. vm2 has historically been seen in SaaS platforms that support user script
execution, online code runners, chatbots, and open-source projects, being used in more than 200,000
projects on GitHub. The project was discontinued in 2023, though, due to repeated sandbox-escape
vulnerabilities, and considered unsafe for running untrusted code."
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/critical-sandbox-escape-flaw-discovered-in-popular-vm2-nodejs-library/

Ivanti Warns Of Two EPMM Flaws Exploited In Zero-Day Attacks

"Ivanti has disclosed two critical vulnerabilities in Ivanti Endpoint Manager Mobile (EPMM), tracked as CVE-2026-1281 and CVE-2026-1340, that were exploited in zero-day attacks. The flaws are codeinjection vulnerabilities that allow remote attackers to execute arbitrary code on vulnerable devices without authentication. Both vulnerabilities have a CVSS score of 9.8 and are rated as critical.
"We are aware of a very limited number of customers whose solution has been exploited at the time of disclosure," warns Ivanti."

https://www.bleepingcomputer.com/news/security/ivanti-warns-of-two-epmm-flaws-exploited-in-zero-day-attacks/

IBM Warns Of Critical API Connect Auth Bypass Vulnerability

"IBM urged customers to patch a critical authentication bypass vulnerability in its API Connect
enterprise platform that could allow attackers to access apps remotely. API Connect is an application programming interface (API) gateway that enables organizations to develop, test, and manage APIs and provide controlled access to internal services for applications, business partners, and external developers. Available in on-premises, cloud, or hybrid deployments, API Connect is used by hundreds of companies in banking, healthcare, retail, and telecommunications sectors."
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/ibm-warns-of-

critical-api-connect-auth-bypass-vulnerability/

configuration-changes-fortinet-fortigate-devices-via-ssoaccounts/

Malware

Arctic Wolf Observes Malicious Configuration Changes On Fortinet FortiGate Devices Via SSO Accounts

"Starting on January 15, 2026, Arctic Wolf began observing a new cluster of automated malicious activity involving unauthorized firewall configuration changes on FortiGate devices. This activity involved the creation of generic accounts intended for persistence, configuration changes granting VPN access to those accounts, as well as exfiltration of firewall configurations. This is a developing situation, and we will share more technical details of this threat with the public as more information becomes available. While the parameters of initial access details have not been fully confirmed, the current campaign bears similarity to a campaign described by Arctic Wolf in December 2025. In the December security bulletin, we provided details of SSO login activity for administrator accounts, followed by configuration changes and exfiltration on affected firewall devices."

https://arcticwolf.com/resources/blog/arctic-wolf-observes-malicious-

RondoDoX Botnet Weaponizes React2Shell

"CloudSEK's report details a persistent nine-month RondoDoX botnet campaign targeting IoT devices and web applications. Recently, the threat actors have shifted to weaponizing a critical Next.js vulnerability, deploying malicious payloads like "React2Shell" and cryptominers. This analysis offers crucial insights into their evolving infrastructure and provides defensive recommendations to mitigate these sophisticated attacks."

https://www.cloudsek.com/blog/rondodox-botnet-weaponizes-react2shell

GlassWorm Goes Mac: Fresh Infrastructure, New Tricks

"Two and a half months ago, we exposed GlassWorm, the first self-propagating worm targeting VS Code extensions, using invisible Unicode characters to hide malicious code. We've tracked this threat actor through three waves: invisible Unicode payloads, a return strike that exposed real victims including a Middle Eastern government entity, and a pivot to compiled Rust binaries. Now they're back. With 50,000 downloads, a platform switch from

Windows to macOS, and the infrastructure is fully operational as you read this."

https://www.koi.ai/blog/glassworm-goes-mac-fresh-infrastructure-new-tricks

Cyber Counterintelligence (CCI): When 'Shiny Objects' Trick 'Shiny Hunters'

"It is worth noting that "Shiny Hunters" (tricked by our team with a honeytrap), or more accurately, their rebranded version involving new members, which calls itself "Scattered Lapsus$ Hunters" (SLH) or "Scattered Lapsus$ Shiny Hunters (SLSH)," linked to 'The Com' (short for 'The Community'), a predominantly English-speaking cybercriminal ecosystem. This loosely organized network operates more like a cybercrime youth movement, encompassing a broad and constantly shifting range of actors, mainly teenagers. Some announcements of successful data breaches by these actors were published on the associated Telegram channel, "The Comm Leaks." The FBI issued a Public Service Announcement (PSA) last year warning about the risks associated with joining such movements."

Advisory

Advisory 117: Microsoft Windows Information Disclosure Vulnerability

CVE-2026-20805 is a security vulnerability in Microsoft Windows' Desktop Window Manager (DWM) where an attacker with local access can disclose sensitive information (memory data) that should be protected. This is classified as an information disclosure flaw, and it was confirmed to be actively exploited in the wild before a patch was issued.

This alert is relevant to Organizations and System/Network administrators that utilize the above products. This alert is intended to be understood by technical users and systems administrators.

https://cert.gov.vu/index.php/advisories/112-advisory-117#what-is-it

Advisory 118: Microsoft Office Security Feature Bypass Vulnerability

CVE-2026-21509 is a high-severity security feature bypass vulnerability in Microsoft Office caused by reliance on untrusted input in security decisions. It allows attackers to bypass built-in protections (e.g., OLE/COM security controls) when a user opens a specially crafted Office document.

This alert is relevant to Organizations and System/Network administrators that utilize the

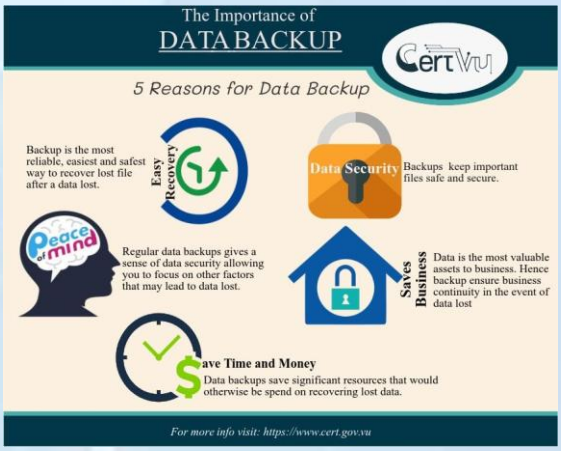
above products. This alert is intended to be understood by technical users and systems administrators.

https://cert.gov.vu/index.php/advisories/113-advisory-118

Advisory 119: Fortinet Multiple Products Authentication Bypass Using an Alternate Path or Channel Vulnerability
CVE-2026-24858 is a critical authentication bypass vulnerability (CWE-288) in Fortinet products.
It allows attackers to bypass FortiCloud Single Sign-On (SSO) authentication using an alternate authentication path, enabling unauthorized access to protected devices.
his alert is relevant to Organizations and System/Network administrators that utilize the above products. This alert is intended to be understood by technical users and systems administrators.

https://cert.gov.vu/index.php/advisories/114-advisory-119

Best Practice and Tips



Source: CERTVU

Upcoming Events

The Digital Roadshow
A digital roadshow is an outreach initiative where an organization brings digital services, tools, and awareness programs directly to communities instead of people traveling to a central event, through demonstrations, training sessions, and engagement activities that promote digital literacy, the use of online services, support for businesses to go digital, and improved cybersecurity awareness.

The 2026 Cyber security Boot Camp
As part of *Digital Week Vanuatu* held every year, a Cybersecurity Boot camp was organized to inspire and equip young people with essential cyber-safety and digital security skills. The boot camp, supported by CERT Vanuatu (CERTVU) and the Department of Communication and Digital Transformation, targeted senior secondary school students with hands-on learning experiences that build awareness

of online threats and introduce cybersecurity fundamentals. It aims to nurture the next generation of cybersecurity leaders in Vanuatu by offering interactive sessions that combine practical exercises with discussions about safe internet use and the importance of protecting digital information. Participants also have the opportunity to earn recognition for their involvement, helping build confidence and interest in careers within the growing ICT and cybersecurity fields.

Cyber month Event

The cyber month Event is scheduled for October, a period dedicated to advancing cybersecurity across the nation.

In line with Cyber Up Pacific, CERTVU (CERT Vanuatu) staff will lead Cyber Week during Cyber Month, focusing on raising cybersecurity awareness across communities, schools, and both private and public agencies.

Source: CERTVU

These efforts aim to educate the public on best practices and promote safe online behaviors, reinforcing Vanuatu's commitment to securing the region's digital future and to strengthen the nation's digital resilience.

CERT Vanuatu Efforts

The ongoing initiatives by CERT Vanuatu (CERT-VU) to advance cybersecurity in Vanuatu are of utmost importance. CERT-VU actively collaborates with diverse stakeholders to address cybersecurity concerns across a range of activities, aiming to cultivate a community that is well-versed in cybersecurity and resilient against cyber-attacks.

Cybersecurity Awareness Program

CERTVU is actively engaged in a range of initiatives as part of our ongoing awareness program. One key avenue for reaching our audience is through Platform Radio Vanuatu's morning shows, where we conduct engaging ICT talks to inform and educate the public.

Source: CERTVU

Additionally, we are leveraging online platforms to distribute awareness materials. Our social media presence, particularly on Facebook at https://www.facebook.com/CERTVU, is a vital channel for reaching a broader audience and fostering dialogue on cybersecurity and related topics.

Multi-stakeholder Initiative

Cloud infrastructure Roadmap and Cyber Security Agency

The Department of Communication and Digital Transformation (DCDT) is actively working with local stakeholders on two pivotal initiatives: the development of a Cloud Infrastructure Roadmap and the establishment of a Cybersecurity Agency.

The **Cloud Infrastructure Roadmap** aims to guide the strategic implementation of cloud technologies across government and public services. By collaborating with local stakeholders, the DCDT is ensuring that the roadmap reflects the needs and capabilities of Vanuatu, facilitating a smooth and effective transition to cloud-based solutions.

In parallel, efforts are underway to establish a **Cybersecurity Agency**. This new agency will play a crucial role in enhancing the country's cybersecurity posture, providing centralized oversight, and developing policies to protect national digital assets. The agency will work closely with various sectors to strengthen Vanuatu's ability to defend against cyber threats and secure its digital environment.

These initiatives reflect the Vanuatu Government's commitment to advancing its digital infrastructure and cybersecurity capabilities, ensuring a secure and resilient future for the country.

Capacity Building Program

CERTVU, dedicated to advancing Knowledge and skills, persistently drives forward with its commitment to promoting and facilitating capacity-building programs. Through sustained collaboration with both national and international partners, CERTVU endeavors to strengthen capacities across various sectors. These partnerships exemplify CERTVU's proactive approach in seeking out strategic alliances to enhance capacity building efforts.

This initiative, designed for critical infrastructure organizations in Vanuatu, took place from Monday, August 26, to Friday, August 30, 2024, at the Ramada Resort by Wyndham in Port Vila.

International Collaboration

CERT Vanuatu (CERT-VU) has been Steadfast in maintaining and strengthening its international collaborations over the years to elevate its position in the global cybersecurity landscape.

PACSON

The Department of Digital Communication and Digital Transformation (DCDT) through CERTVU, plays a continuous role in several key working groups within the Pacific Cyber Security Operational Network (PACSON).

- **Awareness Raising Working Group**: This group focuses on spreading cybersecurity knowledge across the Pacific. One of its key initiatives is the **CyberSmart** awareness materials, which are used to educate the public and organizations about online threats and safe practices.
- **Community Working Group**: This group aims to create a cohesive and resilient cyber community by

promoting best practices and facilitating information sharing among Pacific nations.

- **Capacity Building Working Group**: This group is dedicated to enhancing the region's cybersecurity capabilities by providing targeted training and support to fill knowledge gaps and strengthen skills.

Through its involvement in these groups, the DCDT, via CERTVU, is actively contributing to a stronger, more secure digital environment across the Pacific.

Incident Response

CERTVU operates a proactive incident response team focused on the daily management of prevalent cyber Threats.

The persistent efforts of CERTVU's incident response team play a crucial role in identifying, mitigating, and preventing these threats, ensuring a safer digital environment for individuals and organizations alike.

Through continuous monitoring, training, and awareness programs, CERTVU is committed to reducing the impact of these cyber threats, demonstrating the critical importance of preparedness and resilience in today's digital age.

References

1. https://thehackernews.com/2026/01/critical-wordpress-modular-ds-plugin.html
2. https://thehackernews.com/2026/01/critical-wordpress-modular-ds-plugin.html
3. https://www.bleepingcomputer.com/news/security/hackers-exploit-modular-ds-wordpress-plugin-flaw-for-admin-access/
4. https://www.facebook.com/CERTVU
5. https://patchstack.com/articles/critical-privilege-escalation-vulnerability-in-modular-ds-plugin-affecting-40k-sites-exploitedin-the-wild/
7. https://www.theregister.com/2026/01/15/cisco_fixes_cve_2025_20393/
8. https://blog.checkpoint.com/research/patch-now-active-exploitation-underway-for-critical-hpe-oneview-vulnerability/
9. https://www.theregister.com/2026/01/16/rondodox_botnet_hpe_oneview/
10. https://www.infosecurity-magazine.com/news/rondodox-botnet-targets-hpe/
11. https://www.bleepingcomputer.com/news/security/acf-plugin-bug-gives-hackers-admin-on-50-000-wordpress-sites/
12. https://www.wordfence.com/blog/2026/01/100000-wordpress-sites-affected-by-privilege-escalation-vulnerability-inadvanced-custom-fields-extended-wordpress-plugin/
13. https://www.securityweek.com/oracles-first-2026-cpu-delivers-337-new-security-patches/
14. https://thehackernews.com/2026/01/zoom-and-gitlab-release-security.html
15. https://www.bleepingcomputer.com/news/security/gitlab-warns-of-high-severity-2fa-bypass-denial-of-service-flaws/
16. https://securityaffairs.com/187165/security/zoom-fixed-critical-node-multimedia-routers-flaw.html
17. https://thehackernews.com/2026/01/critical-gnu-inetutils-telnetd-flaw.html
18. https://www.theregister.com/2026/01/22/root_telnet_bug/
19. https://patchstack.com/articles/critical-arbitrary-file-upload-vulnerability-in-realhomes-crm-plugin-affecting-30k-sites/
20. https://www.infosecurity-magazine.com/news/realhomes-crm-plugin-flaw/
21. https://www.bleepingcomputer.com/news/security/critical-sandbox-escape-flaw-discovered-in-popular-vm2-nodejs-library/
22. https://www.bleepingcomputer.com/news/security/ivanti-warns-of-two-epmm-flaws-exploited-in-zero-day-attacks/
23. https://forums.ivanti.com/s/article/Security-Advisory-Ivanti-Endpoint-Manager-Mobile-EPMM-CVE-2026-1281-CVE-2026-1340?language=en_US

24. https://arcticwolf.com/resources/blog/arctic-wolf-observes-malicious-configuration-changes-fortinet-fortigate-devices-via-ssoaccounts/
25. https://thehackernews.com/2026/01/automated-fortigate-attacks-exploit.html
26. https://www.bleepingcomputer.com/news/security/hackers-breach-fortinet-fortigate-devices-steal-firewall-configs/
27. https://www.darkreading.com/cloud-security/fortinet-firewalls-malicious-configuration-changes
28. https://securityaffairs.com/187194/hacking/arctic-wolf-detects-surge-in-automated-fortinet-fortigate-firewall-configurationattacks.html
29. https://www.securityweek.com/new-wave-of-attacks-targeting-fortigate-firewalls/
30. https://www.theregister.com/2026/01/22/fortigate_firewalls_hit_by_silent/
31. https://www.bleepingcomputer.com/news/security/ibm-warns-of-critical-api-connect-auth-bypass-vulnerability/
32. https://www.ibm.com/support/pages/node/7255149
33. https://thehackernews.com/2025/12/ibm-warns-of-critical-api-connect-bug.html
34. https://www.cloudsek.com/blog/rondodox-botnet-weaponizes-react2shell
35. https://www.bleepingcomputer.com/news/security/rondodox-botnet-exploits-react2shell-flaw-to-breach-nextjs-servers/
36. https://www.koi.ai/blog/glassworm-goes-mac-fresh-infrastructure-new-tricks
37. https://www.bleepingcomputer.com/news/security/new-glassworm-malware-wave-targets-macs-with-trojanized-cryptowallets/
38. https://www.resecurity.com/blog/article/cyber-counterintelligence-cci-when-shiny-objects-trick-shiny-hunters
39. https://databreaches.net/2026/01/06/cyber-counterintelligence-cci-resecurity-releases-data-on-john-erin-binns-irdev/

