



[TLP: CLEAR]

Monthly Security Bulletin– May 2026

Overview

Regards,

CERT Vanuatu (CERTVU), a unit within the Department of Communication and Digital Transformation (DCDT), is pleased to share its Monthly Security Bulletin. This edition provides an overview of significant vulnerabilities and actively exploited threats identified during May 2026 across commonly used systems and applications. The bulletin aims to assist organizations in enhancing their cybersecurity awareness, preparedness, and resilience against emerging cyber risks.

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

MetInfo CMS CVE-2026-29014 Exploited For Remote Code Execution Attacks

"Threat actors are actively exploiting a critical security flaw impacting an open-source content management system (CMS) known as MetInfo, according to new findings from VulnCheck. The vulnerability in question is CVE-2026-29014 (CVSS score: 9.8), a code injection flaw that could result in arbitrary code execution. "MetInfo CMS versions 7.9, 8.0, and 8.1 contain an unauthenticated PHP code injection vulnerability that allows remote attackers to execute arbitrary code by sending crafted requests with malicious PHP code," the NIST National Vulnerability Database (NVD) states."

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

mitigation steps to mitigate these vulnerabilities.

<https://thehackernews.com/2026/05/metinfo-cms-cve-2026-29014-exploited.html>

Critical cPanel And WHM Bug Exploited As a Zero-Day, PoC Now Available

"The critical CVE-2026-41940 authentication bypass vulnerability in cPanel, WHM, and WP Squared is being actively exploited in the wild and has been leveraged in attempts since late February. It is unclear when exploitation started, but KnownHost, a hosting provider that uses cPanel, said the day the vulnerability was disclosed that "successful exploits have been seen in the wild" before a fix became available. However, KnownHost CEO Daniel Pearson stated that the company has "seen execution attempts as early as 2/23/2026." 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-cpanel-and-whm-bug-exploited-as-a-zero-day-poc-now-available/>

A CVSS 10.0 In Gemini CLI: How Agentic Workflows Are Reshaping Supply Chain Risk

"The flaw lived in how Gemini CLI handled workspace trust in non-interactive environments. When running in headless mode – like a CI/CD job – Gemini CLI automatically trusted the current workspace folder, loading any agent configuration it found there without review, sandboxing, or human approval. That meant an attacker who could place content in a repository's workspace – by opening a pull request, for example – could plant configuration that the agent would silently trust and act on. The result was direct command execution on the host running the agent, before its sandbox ever initialized. Across every affected workflow, the impact was the same: code execution on the host running the agent gave an unprivileged outsider access to whatever secrets, credentials, and source code the workflow could reach. Enough for token theft, supply-chain pivots, and lateral movement into downstream systems."

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

<https://novee.security/blog/google-gemini-cli-rce-vulnerability-cvss-10-critical-security-advisory/>

Critical Vm2 Sandbox Bug Lets Attackers Execute Code On Hosts

"A critical vulnerability in the popular Node.js sandboxing library vm2 allows escaping the sandbox and executing arbitrary code on the host system. The security issue is tracked as CVE-2026-26956 and has been confirmed to impact vm2 version 3.10.4, although earlier releases may also be vulnerable. Proof of-concept (PoC) exploit code has been published. In the security advisory, the maintainer says that the issue only impacts environments with Node.js 25 (confirmed on Node.js 25.6.1) that have enabled WebAssembly exception handling and JSTag support."

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/critical-vm2-sandbox-bug-lets-attackers-execute-code-on-hosts/>

Palo Alto Networks Warns Of Firewall RCE Zero-Day Exploited In Attacks

"Palo Alto Networks warned customers today that a critical-severity unpatched vulnerability in the PAN OS User-ID Authentication Portal is being exploited in attacks.

Also known as the Captive Portal, the User-ID Authentication Portal is a PAN-OS security feature that authenticates users whose identities cannot be automatically mapped by the firewall. Tracked as CVE-2026-0300, this zero-day bug stems from a buffer overflow weakness that allows unauthenticated attackers to execute arbitrary code with root privileges on Internet-exposed PA-Series and VM-Series firewalls via specially crafted packets."

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/palo-alto-networks-warns-of-actively-exploited-firewall-zero-day/>

Cross The Cline

"Cline is one of the most widely adopted open-source AI coding agents. Developers trust it with deep access to their environments: source code, terminals, git repositories, cloud credentials, and, increasingly, agent autonomy that lets it act on their behalf without per-step confirmation. That trust comes with a critical assumption: only the developer, through Cline's own UI, can communicate with the agent. Oasis Security researchers found a critical vulnerability (CVSS 9.7) in Cline's local kanban server.

Any website a developer visited while running an affected version could silently connect to their machine, exfiltrate workspace data in real time, and inject commands into the developer's AI agent. The developer would see nothing unusual. They were just browsing the web."

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

<https://www.oasis.security/blog/clone-kanban-websocket-hijack>

My Agentic Trust Issues: From Prompt Injection To Supply-Chain Compromise On Gemini-Cli

"Pillar Security researchers identified a CVSS 10 critical vulnerability (dubbed TrustIssues) in Google's AI powered GitHub workflows that allowed any external attacker, with nothing more than a public GitHub issue, to a full supply chain compromise of the gemini-cli repository, Google's AI coding agent with 101,000+ stars. The critical severity rating reflects a specific bypass our researcher Dan Lisichkin identified inside Gemini CLI itself. The strategic impact is what that vulnerability enabled: a complete supply-chain compromise of Google's gemini-cli repository."

CERTVU recommends all users and organizations to read this

Vulnerability and follow the mitigation steps to mitigate these vulnerabilities.

<https://www.pillar.security/blog/my-agentic-trust-issues-from-prompt-injection-to-supply-chain-compromise-on-gemini-cli>

SAP Fixes Critical Vulnerabilities In Commerce Cloud And S/4HANA

"SAP has released the May 2026 security updates addressing 15 vulnerabilities across multiple products, including two critical flaws in Commerce Cloud and S/4HANA. Commerce Cloud is an enterprise-grade e-commerce platform used by online stores owned by large retailers and global brands, while S/4HANA is a cloud-based Enterprise Resource Planning (ERP) suite that will replace the company's on-premises ECC ERP system. Tracked as CVE-2026-34263, the first critical flaw is a missing authentication check in SAP Commerce Cloud that allows unauthenticated attackers to execute code on vulnerable servers."

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/sap-fixes-critical-vulnerabilities-in-commerce-cloud-and-s-4hana/>

Adobe Patches 52 Vulnerabilities In 10 Products

"Adobe on Tuesday announced the release of patches for 52 vulnerabilities across 10 products, including critical-severity bugs that could lead to code execution and privilege escalation. More than half of the weaknesses Adobe addressed this month could be exploited for arbitrary code execution. Application denial-of-service (DoS) was the second most common type of resolved issue. When it comes to the severity of the resolved vulnerabilities, the AdobeConnect update takes the lead. It addresses two critical-severity flaws that could be exploited for arbitrary code execution (CVE-2026-34659, CVSS score of 9.6) and privilege escalation (CVE-2026-34660, CVSS score of 9.3)."

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-52-vulnerabilities-in-10-products/>

New Exim BDAT Vulnerability Exposes GnuTLS Builds To Potential Code Execution

"Exim has released security updates to address a severe security issue affecting certain

configurations that could enable memory corruption and potential code execution. Exim is an open-source Mail Transfer Agent (MTA) designed for Unix-like systems to receive, route, and deliver email. The vulnerability, tracked as CVE-2026-45185, aka Dead.Letter, has been described as a use-after-free vulnerability in Exim's binary data transmission (BDAT) message body parsing when a TLS connection is handled by GnuTLS."

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

<https://thehackernews.com/2026/05/new-exim-bdat-vulnerability-exposes.html>

CVE-2025-32975: The Open Directory Behind The KACE SMA Breach And 60+ Downstream Victims

"Quest KACE Systems Management Appliance (SMA) is a widely deployed on-premises platform that enterprises use for endpoint management, handling software deployment, patch distribution, inventory, and scripted administrative control across managed devices. That privileged position makes it an exceptionally high-value target for an attacker who controls a KACE SMA appliance, which, in many environments, can reach every

managed endpoint from a single trusted management plane. CVE-2025 32975 is a critical authentication bypass vulnerability in KACE SMA's SSO authentication handling mechanism with a CVSS score of 10.0. The flaw allows an unauthenticated, network-reachable attacker to impersonate legitimate users, including administrators, without supplying any credentials."

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

<https://hunt.io/blog/cve-2025-32975-quest-kace-sma-open-directory-60-victims>

Fortinet, Ivanti Patch Critical Vulnerabilities

"Fortinet and Ivanti on Tuesday announced patches for 18 vulnerabilities across their product portfolios, including three critical-severity bugs. Fortinet published 11 advisories describing as many bugs, including two dealing with critical-severity code execution security defects. Tracked as CVE-2026-44277 (CVSS score of 9.1), the first of them is an improper access control issue in FortiAuthenticator that could be exploited remotely, without authentication, via crafted requests. "FortiAuthenticator Cloud is not impacted by the issue, and hence customers do not need

to perform any action," the company says."

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

<https://www.securityweek.com/fortinet-ivanti-patch-critical-vulnerabilities/>

200,000 WordPress Sites At Risk From Critical Authentication Bypass Vulnerability In Burst Statistics Plugin

"On May 8, 2026, PRISM, Wordfence Threat Intelligence's autonomous vulnerability research platform, discovered a critical Authentication Bypass vulnerability in Burst Statistics, a WordPress plugin with more than 200,000 active installations. The vulnerability was introduced in the code on April 23, 2026, discovered just 15 days later, and patched 19 days later, highlighting the positive impact that AI can have on reducing the window for attackers to find and target new vulnerabilities in WordPress. This vulnerability allows unauthenticated attackers who know a valid administrator username to fully impersonate that administrator for the duration of any REST API request, including WordPress core endpoints such as /wp-json/wp/v2/users, by supplying any arbitrary and incorrect password in a Basic

Authentication header. In a worst-case scenario, an attacker could exploit this flaw to create a new administrator-level account with no prior authentication whatsoever."

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

<https://www.wordfence.com/blog/2026/05/200000-wordpress-sites-at-risk-from-critical-authentication-bypass-vulnerabilityin-burst-statistics-plugin/>

Ongoing Exploitation Of Cisco Catalyst SD-WAN Vulnerabilities

"Cisco Talos is tracking the active exploitation of CVE-2026-20182, an authentication bypass vulnerability in Cisco Catalyst SD-WAN Controller, formerly SD-WAN vSmart, and Cisco Catalyst SD-WAN Manager, formerly SD-WAN vManage. Successful exploitation of CVE-2026-20182 allows an unauthenticated, remote attacker to bypass authentication and obtain administrative privileges on an affected system. The exploitation of CVE-2026-20182 appears to have been limited so far and Talos clusters this activity under UAT-8616 with high confidence."

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

mitigation steps to mitigate these vulnerabilities.

<https://blog.talosintelligence.com/sd-wan-ongoing-exploitation/>

Malware

FortiClient EMS Exploited Via CVE-2026-35616 To Deliver EKZ Infostealer Disguised As a Fortinet Patch

"In May 2026, Arctic Wolf observed a cluster of malicious activity affecting endpoints managed by FortiClient Endpoint Management Server (EMS). The malicious payload was disguised as a fake Fortinet endpoint patch, but it was actually a credential stealer. We named this payload EKZ Infostealer, based on internal symbol names extracted from decrypted code. This infostealer, which primarily targets browser-based credentials, stages its harvested results in a log file and exfiltrates obtained credentials over HTTP."

<https://thehackernews.com/2026/05/threat-actors-exploit-critical.html>

Nx Console VS Code Extension Compromised

"On May 18, 2026, a compromised version of the Nx Console VS Code extension (nrwl.angular-console v18.95.0) was published to the

Visual Studio Code Marketplace. The extension has over 2.2 million installations. Within seconds of a developer opening any workspace, the compromised extension silently fetched and executed a 498 KB obfuscated payload from a dangling orphan commit hidden inside the official nrwl/nx GitHub repository. If you have this version installed, assume your system is compromised. The payload is a multi-stage credential stealer and supply chain poisoning tool. It harvests tokens and secrets from GitHub, npm, AWS, HashiCorp Vault, Kubernetes, and 1Password, then exfiltrates them over three independent channels: HTTPS, the GitHub API, and DNS tunneling. It also installs a persistent Python backdoor on macOS that uses the GitHub Search API as a dead-drop for receiving further commands signed with a 4096-bit RSA key."

<https://www.stepsecurity.io/blog/nx-console-vs-code-extension-compromised>

Critical cPanel Flaw Mass-Exploited In "Sorry" Ransomware Attacks

"A new disclosed cPanel flaw tracked as CVE-2026-41940 is being mass-exploited to breach websites and encrypt data in "Sorry" ransomware attacks. This week, an emergency update for WHM and cPanel was released to fix a critical authentication bypass flaw that

allows attackers to access control panels. WHM and cPanel are Linux-based web hosting control panels for server and website management. While WHM provides server-level control, cPanel provides administrator access to the website backend, webmail, and databases. Soon after its release, it was reported that the flaw was being actively exploited in the wild as a zero-day, with exploitation attempts dating back to late February."

<https://www.bleepingcomputer.com/news/security/critical-cpanel-flaw-mass-exploited-in-sorry-ransomware-attacks/>

CERTVU Threat Statistics

The Attack Index is a daily composite score (0–100) calculated by TrendAI Vision One™ based on the number and severity of unique threat detections within the monitored environment and the volume of impacted assets. A score above 60 indicates an elevated threat environment; above 80 indicates critical-level attack intensity.

46.4 Opening Index - 2 May	82.2 Peak Index - 18 May	66.1 Month Average Index	70.7 Closing Index - 30 May
5 Days Index > 80 (Critical)	12 Days Index > 70 (High)	11 of 13 MITRE Phases Active	+52% Index Rise: Open vs Close

Key observations:

- The attack index remained above 60 for the entire period from 10 May to 30 May — 21 consecutive elevated days.

- The index crossed the critical threshold of 80 on five dates: 15 May (79.6), 16 May (80.9), 17 May (80.0), 18 May (82.2), and 21 May (80.2).
- Despite a brief decline in week 4 (64–72 range), the index never returned below the elevated threshold of 60 for the remainder of the month.
- The closing index of 70.7 on 30 May confirms that elevated attack pressure persisted through the final day of the reporting period.

CERTVU Advisories

Advisory 146: Microsoft Defender Denial of Service Vulnerability

CVE-2026-45498 is a medium-severity Denial of Service (DoS) vulnerability (CVSS 4.0) affecting Microsoft Defender and the Microsoft Malware Protection Engine. The vulnerability allows an attacker to cause the security service to become unavailable or unstable through local exploitation.

<https://cert.gov.vu/index.php/advisories/155-advisory-146>

Advisory 145: Microsoft Internet Explorer Use-After-Free Vulnerability

CVE-2010-0249 is a critical remote code execution (RCE) vulnerability in Microsoft Internet Explorer. The flaw is caused by a memory corruption/use-after-free

vulnerability in the way Internet Explorer handles certain HTML objects and cascading style sheets. When a user visits a specially crafted malicious webpage, Internet Explorer may improperly access freed memory, allowing attackers to execute arbitrary code on the victim's system.

<https://cert.gov.vu/index.php/advisories/154-advisory-145>

Advisory 144: Adobe Acrobat and Reader Heap-Based Buffer Overflow Vulnerability

CVE-2009-3459 is a critical remote code execution (RCE) vulnerability affecting Adobe Reader and Adobe Acrobat.

The vulnerability is caused by a buffer overflow and memory corruption flaw in the handling of specially crafted PDF files containing embedded JavaScript and malformed objects.

<https://cert.gov.vu/index.php/advisories/153-advisory-144>

Advisory 143: Microsoft Exchange Server Cross-Site Scripting Vulnerability

CVE-2008-4250 is a critical remote code execution (RCE) vulnerability in the Microsoft Windows Server Service. The flaw is caused by an improperly handled RPC request

resulting in a stack-based buffer overflow.

The vulnerability became widely known through exploitation by the Conficker worm and is associated with Microsoft Security Bulletin MS08-067

<https://cert.gov.vu/index.php/advisories/152-advisory-14>

Advisory 142: Microsoft Exchange Server Cross-Site Scripting Vulnerability

CVE-2026-44277 is a critical vulnerability (CVSS 9.8) affecting Fortinet FortiAuthenticator. The flaw is classified as an improper access control vulnerability (CWE-284).

<https://cert.gov.vu/index.php/advisories/151-advisory-143>

Advisory 141: Microsoft Exchange Server Cross-Site Scripting Vulnerability

CVE-2026-42897 is a high-severity reflected Cross-Site Scripting (XSS) vulnerability affecting the Outlook on the web (OWA) component of Microsoft Exchange Server. The flaw stems from improper neutralization of user-supplied input during web page generation. Discovered as a zero-day and actively exploited in the wild, the vulnerability allows unauthenticated attackers to execute arbitrary JavaScript within

the security context of a targeted user's session, facilitating session hijacking and identity spoofing. Microsoft confirms it had detected active exploitation of this vulnerability in the wild.

<https://cert.gov.vu/index.php/advisories/150-advisory-142>

These alerts are 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.

Events

Digital Week Vanuatu 2026

Digital Week Vanuatu 2026 was held from **13 to 15 May 2026 at Independence Park in Port Vila**, bringing together government, private sector, schools, communities, and other stakeholders to promote digital transformation and innovation. The event highlighted the importance of reliable, inclusive, and resilient digital technologies in supporting communities, essential services, and national development.

CERT Vanuatu (CERTVU) actively contributed to the event by establishing a **cybersecurity awareness booth**, where members of the public, students, and other participants could access

information and guidance on cybersecurity, online safety, and protecting personal information. The booth provided an opportunity for CERTVU to engage directly with the community, answer cybersecurity-related questions, and promote safe and responsible use of digital technologies as part of its broader national cybersecurity awareness mandate.



Source: CERTVU

The 2026 Cyber security Boot Camp Cybersecurity Boot Camp



Source: CERTVU

As part of the annual **Digital Week Vanuatu**, a Cybersecurity Boot Camp was conducted on **14 and 15 May 2026** to raise cybersecurity awareness among young people and introduce them to the fundamentals of digital security.

The two-day program was supported by **CERT Vanuatu (CERTVU)** and the **Department of Communication and Digital Transformation (DCDT)** and was specifically designed for senior secondary school students. The boot camp provided participants with an opportunity to gain practical knowledge and develop a better understanding of common online threats, cybersecurity risks, and safe digital practices.

Through interactive presentations, practical exercises, discussions, and cybersecurity activities, participants were encouraged to think critically about their online safety and the importance of protecting personal and digital information. The program also provided students with an introduction to cybersecurity as a potential career pathway and helped strengthen their interest in ICT and digital security.

The Cybersecurity Boot Camp forms part of CERTVU's broader efforts to build cybersecurity awareness and develop the next generation of digitally responsible and cybersecurity-conscious young people in Vanuatu.

Cyber Month Event

October is observed as **Cyber Month**, a national awareness initiative aimed at promoting safe and responsible use of digital technologies while strengthening

cybersecurity awareness and resilience throughout Vanuatu.

As part of the **Cyber Up Pacific** campaign, CERT Vanuatu (CERTVU) coordinates a range of **Cyber Week activities** involving communities, schools, government institutions, businesses, and other stakeholders. These activities include cybersecurity awareness sessions, community outreach, educational programs, and capacity-building initiatives.

The overall objective is to increase public understanding of cyber threats, encourage good cybersecurity practices, and empower individuals and organizations to better protect their information, systems, and digital services. Through these activities, CERTVU continues to contribute to building a stronger, safer, and more resilient digital environment across Vanuatu.

CERTVU Efforts

CERT Vanuatu (CERTVU) continues to support the development of cybersecurity in Vanuatu. The team works with government agencies, businesses, communities, schools, and international partners to improve cybersecurity awareness, build skills, and help prevent and respond to cyber threats.

Cybersecurity Awareness Program

CERTVU continues to conduct cybersecurity awareness activities for the public. One of the main ways the team reaches people is through **Platform Radio Vanuatu morning programs**, where CERTVU delivers ICT and cybersecurity talks on topics such as online safety, cyber threats, and protecting personal information.

Online Cybersecurity Awareness

CERTVU also uses social media and other online platforms to share cybersecurity information with the public. Awareness materials, updates, alerts, and safety tips are regularly published to encourage people to use digital services safely. The **CERTVU Facebook page** is an important platform for reaching a wider audience. It also allows the team to share information about current cyber threats and interact with the public on cybersecurity matters.

Multi-Stakeholder Initiatives Cloud Infrastructure Roadmap and Cybersecurity Agency

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

The Cloud Infrastructure Roadmap will provide guidance on the use of

cloud technology across government and public services. It will help ensure that cloud services are introduced in a safe, planned, and effective way.

The proposed Cybersecurity Agency will strengthen national cybersecurity by providing greater coordination, oversight, policy development, and support for protecting Vanuatu's digital systems and services.

These initiatives demonstrate the Government's commitment to strengthening Vanuatu's digital infrastructure and improving national cybersecurity.

Capacity Building Program

CERTVU continues to focus on building cybersecurity knowledge and skills across different sectors. The team works with local and international partners to provide training and other capacity-building opportunities.

One of the key programs was a capacity-building activity for **critical infrastructure organizations in Vanuatu**, held from **26 to 30 August 2024 at the Ramada Resort by Wyndham in Port Vila**. The program provided participants with knowledge and practical skills to better understand and manage cybersecurity risks.

International Collaboration

CERTVU continues to work with regional and international partners

to strengthen Vanuatu's cybersecurity capabilities. These partnerships provide opportunities for knowledge sharing, training, technical support, and participation in regional cybersecurity initiatives.

Pacific Cyber Security Operational Network (PaCSON)

Through DCDT, CERTVU continues to participate in several working groups under the **Pacific Cyber Security Operational Network (PaCSON)**. These include:

- **Awareness Raising Working Group** – focuses on improving cybersecurity awareness across the Pacific, including the use of **CyberSmart** awareness materials.
- **Community Working Group** – promotes cooperation, information sharing, and good cybersecurity practices among Pacific countries.
- **Capacity Building Working Group** – supports training and skills development to address cybersecurity knowledge gaps across the region.

CERTVU's participation in these working groups helps strengthen cooperation and contributes to a safer and more resilient digital environment in Vanuatu and across the Pacific.

Incident Response

CERTVU has an incident response team that helps monitor, manage, and respond to cybersecurity incidents affecting individuals and organizations.

The team works to identify and respond to threats such as **phishing, malware, ransomware, and other cyber incidents**. Through incident response, monitoring, training, and public awareness, CERTVU helps reduce the impact of cyber threats and promotes better cybersecurity preparedness across Vanuatu.

References

1. <https://blog.talosintelligence.com/sd-wan-ongoing-exploitation/>
2. <https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sdwan-rpa2-v69WY2SW>
3. <https://www.bleepingcomputer.com/news/security/cisco-warns-of-new-critical-sd-wan-flaw-exploited-in-zero-day-attacks/>
4. <https://www.darkreading.com/vulnerabilities-threats/maximum-severity-cisco-sd-wan-bug-exploited>
5. <https://thehackernews.com/2026/05/cisco-catalyst-sd-wan-controller-auth.html>
7. <https://www.securityweek.com/fortinet-ivanti-patch-critical-vulnerabilities/>
8. <https://hunt.io/blog/cve-2025-32975-quest-kace-sma-open-directory-60-victims>
9. <https://securityaffairs.com/192067/security/quest-kace-sma-flaw-cve-2025-32975-when-one-unpatched-tool-opens-the-doorto-60-organizations.html>
10. <https://www.bleepingcomputer.com/news/security/sap-fixes-critical-vulnerabilities-in-commerce-cloud-and-s-4hana/>
11. <https://support.sap.com/en/my-support/knowledge-base/security-notes-news/may-2026.html>
12. <https://www.securityweek.com/sap-patches-critical-s-4hana-commerce-vulnerabilities/>
13. <https://www.securityweek.com/adobe-patches-52-vulnerabilities-in-10-products/>
14. <https://thehackernews.com/2026/05/new-exim-bdat-vulnerability-exposes.html>
15. <https://www.exim.org/static/doc/security/EXIM-Security-2026-05-01.1/EXIM-Security-2026-05-01.1.txt>
16. <https://www.oasis.security/blog/cline-kanban-websocket-hijack>
17. <https://www.infosecurity-magazine.com/news/cline-kanban-websocket-hijack-ai/>
18. <https://www.pillar.security/blog/my-agentic-trust-issues-from-prompt-injection-to-supply-chain-compromise-on-gemini-cli>
19. <https://www.securityweek.com/gemini-cli-vulnerability-could-have-led-to-code-execution-supply-chain-attack/>
20. <https://www.bleepingcomputer.com/news/security/palo-alto-networks-warns-of-actively-exploited-firewall-zero-day/>
21. <https://unit42.paloaltonetworks.com/captive-portal-zero-day/>
22. <https://security.paloaltonetworks.com/CVE-2026-0300>
23. <https://thehackernews.com/2026/05/palo-alto-pan-os-flaw-under-active.html>
24. <https://therecord.media/palo-alto-warns-of-critical-software-bug-firewalls>
25. <https://www.bankinfosecurity.com/palo-alto-firewalls-being-exploited-no-patch-yet-available-a-31612>
26. <https://cyberscoop.com/palo-alto-networks-pan-os-firewall-zero-day-vulnerability-exploited/>

27. <https://www.securityweek.com/palo-alto-networks-to-patch-zero-day-exploited-to-hack-firewalls/>
28. <https://securityaffairs.com/191748/security/palo-alto-networks-pan-os-flaw-exploited-for-remote-code-execution.html>
29. <https://www.bleepingcomputer.com/news/security/critical-vm2-sandbox-bug-lets-attackers-execute-code-on-hosts/>
30. <https://github.com/patriksimek/vm2/security/advisories/GHSA-ffh4-j6h5-pg66>
31. <https://novee.security/blog/google-gemini-cli-rce-vulnerability-cvss-10-critical-security-advisory/>
32. <https://thehackernews.com/2026/04/google-fixes-cvss-10-gemini-cli-ci-rce.html>
33. <https://www.securityweek.com/critical-gemini-cli-flaw-enabled-host-code-execution-supply-chain-attacks/>
34. <https://www.theregister.com/2026/04/30/googles-fix-for-critical-gemini/>
35. <https://www.bleepingcomputer.com/news/security/critical-cpanel-and-whm-bug-exploited-as-a-zero-day-poc-now-available/>
37. <https://www.cisa.gov/news-events/alerts/2026/04/30/cisa-adds-one-known-exploited-vulnerability-catalog>
38. <https://cyberscoop.com/cpanel-authentication-bypass-vulnerability-cve-2026-41940-exploited/>
39. <https://www.securityweek.com/critical-cpanel-whm-vulnerability-exploited-as-zero-day-for-months/>
40. <https://www.theregister.com/2026/04/30/cpanel-wnh-cves/>
41. <https://thehackernews.com/2026/05/metinfo-cms-cve-2026-29014-exploited.html>
42. <https://www.securityweek.com/metinfo-weaver-e-cology-vulnerabilities-in-attackers-crosshairs/>
43. <https://www.facebook.com/CERTVU>

