[TLP: CLEAR]

Monthly Security Bulletin– June 2026

Overview

Greetings,

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 June 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

1-Click RCE In Flowise (CVE-2026-40933): When Is Stdio MCP Actually a Vulnerability?

"Security researchers at Obsidian Security discovered a one-click RCE in Flowise (CVE-2026-40933), an open-source platform for building LLM workflows and AI agents with over 52k GitHub stars. An attacker can fully compromise a server by convincing an authorized user to import a crafted chatflow. Import alone is enough to trigger arbitrary server-side code execution."

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

https://www.obsidiansecurity.com/blog/when-is-stdio-mcp-actually-a-vulnerability

15,000 WordPress Sites Affected By Administrator Account Creation

Vulnerability In WP Maps Pro WordPress Plugin

"On March 24th, 2026, we received a submission for an Unauthenticated Administrator Account Creation vulnerability in WP Maps Pro, a WordPress plugin with more than 15,000 sales. This vulnerability makes it possible for unauthenticated attackers to create new administrator accounts on the affected sites, leading to complete site takeover."
CERTVU recommends all users and organizations to read this vulnerability and follow the mitigation steps to mitigate these vulnerabilities.

https://www.wordfence.com/blog/2026/05/15000-wordpress-sites-affected-by-administrator-account-creation-vulnerability-in-wp-maps-pro-wordpress-plugin/

Critical Windows Netlogon RCE Flaw Now Exploited In Attacks

"The Centre for Cybersecurity Belgium (CCB), the country's national authority for cybersecurity, warned on Friday that threat actors are now exploiting a recently patched critical Windows Netlogon vulnerability in attacks. Netlogon is a remote procedure call (RPC) interface and a core Microsoft Windows Server background service that authenticates services and users on Windows domain-based networks. Microsoft patched this vulnerability (CVE-2026-41089) during the May 2026 Patch Tuesday, describing it as a stack-based buffer overflow in Windows Netlogon that allows attackers without privileges to gain remote code execution on targeted domain controllers."
CERTVU recommends all users and organizations to read this advisory and follow the mitigation steps to mitigate these vulnerabilities.

https://www.securityweek.com/critical-windows-netlogon-vulnerability-in-attackers-crosshairs/

Unauthenticated Privilege Escalation Vulnerability Patched In Kirki WordPress Plugin

"On May 4th, 2026, we received a submission for an Unauthenticated Privilege Escalation vulnerability in the Kirki WordPress plugin. Although the plugin has more than 500,000 active installations, we estimate that only around 150,000 sites are using a vulnerable version, as the issue was introduced in the 6.0 major release. This vulnerability makes it possible for unauthenticated attackers to take over arbitrary user accounts on the site, including administrator accounts, by leveraging the plugin's password reset functionality to have the password reset link delivered to an attacker-controlled email address."

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-kirki-flaw-exploited-to-hijack-wordpress-admin-accounts/

Acer Working To Patch Max Severity Zero-Days In Wave 7 Routers

"Acer confirmed that it's working to address two maximum-severity zero-day vulnerabilities affecting its Wave 7 mesh routers. According to a Friday security advisory, the two security flaws were reported by security researcher Gergo Pap and affect Wave 7 routers running firmware version T7c_GBL_1.01.000055 or earlier. The first zero-day, a broken access control vulnerability tracked as CVE-2026-49200, can allow unauthenticated attackers to remotely access plaintext credentials stored in log archives."
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/acer-warns-of-max-severity-zero-days-affecting-wave-7-routers/

Attackers Actively Exploiting Critical Vulnerability In Everest Forms Pro Plugin

"On March 30th, 2026, we publicly disclosed a critical Remote Code Execution vulnerability in Everest Forms Pro, a WordPress plugin with an estimated 4,000 active installations. This vulnerability can be leveraged by unauthenticated attackers to execute arbitrary PHP code on the server, leading to complete site compromise. The vendor released the fully patched version on March 18th, 2026. Our records indicate that attackers started exploiting the issue on April 13th, 2026. The Wordfence Firewall has already blocked over 29,300 exploit attempts targeting this vulnerability."
CERTVU recommends all users and organizations to read this Vulnerability and follow the mitigation steps to mitigate these vulnerabilities.

https://www.infosecurity-magazine.com/news/everest-forms-pro-rce-actively/

Chrome 149 Patches 429 Vulnerabilities

"Google this week promoted Chrome 149 to the stable channel with patches for 429 vulnerabilities, a record for a single Chrome refresh. Already exceeding several times the total number of Chrome security fixes released in 2025, the

surge in Chrome flaws is likely driven by AI use, which led Google to lower Chrome bug bounties in April. Over 100 of the newly resolved security defects are critical and high-severity issues, most of which are use-after-free and insufficient validation of untrusted input flaws."
CERTVU recommends all users and organizations to read this Vulnerability and follow the mitigation steps to mitigate these vulnerabilities.

https://www.securityweek.com/chrome-149-patches-429-vulnerabilities/

Popping Root On UniFi OS Server: Unauthenticated RCE Chain Detection & Analysis

"Ubiquiti's Security Advisory Bulletin 064 covers vulnerabilities across the UniFi OS device family that chain into unauthenticated remote code execution. An attacker bypasses the front-end authentication gateway to reach an internal API endpoint that runs an attacker-controlled value as a shell command, all without credentials. We confirmed the full chain end-to-end, turning a single request into a reverse shell with full root privileges. The severity comes from what the appliance controls: it is the management plane for the network it runs. Root on it, therefore, exposes every stored secret, lets an attacker forge admin sessions that survive the patch, and, in physical deployments, can compromise managed devices including door controls and security cameras."
CERTVU recommends all users and organizations to read this Vulnerability and follow the mitigation steps to mitigate these vulnerabilities.

https://bishopfox.com/blog/popping-root-on-unifi-os-server-unauthenticated-rce-chain-detection-analysis

SAP Patches Critical NetWeaver, Commerce Vulnerabilities

"Enterprise software maker SAP on Tuesday released 15 new security notes, including four that resolve critical-severity vulnerabilities in NetWeaver, Commerce, and Data Hub. The most severe of the resolved bugs is CVE-2026-44748 (CVSS score of 9.9), described as an XML Signature Wrapping issue in the SAML Authentication of NetWeaver AS ABAP and ABAP Platform. An authenticated attacker with normal privileges could "obtain a valid signed message and send modified signed XML documents with tampered identity information to the verifier," application security firm Onapsis explains."
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-netweaver-commerce-vulnerabilities/

Adobe Patches 123 Vulnerabilities

"Adobe's latest Patch Tuesday updates fix 123 vulnerabilities across 11 products. Of the total, 57 vulnerabilities were patched in Adobe Experience Manager. The vast majority are XSS flaws that allow arbitrary code execution, and three issues have been described as improper input validation that can lead to a security feature bypass. Two critical issues with a CVSS score of 10, both allowing arbitrary code execution, have been patched in Adobe Campaign Classic."
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-123-vulnerabilities/

Ivanti: Max Severity Sentry Flaw Allows Code Execution As Root

"Security software company Ivanti has released patches to address two critical vulnerabilities in its Sentry secure mobile gateway solution, including a maximum-severity flaw that enables remote attackers to execute code with root privileges. Formerly known as MobileIron Sentry, Ivanti Sentry is a security gateway appliance that secures traffic between back-end corporate systems and remote mobile devices. Tracked as CVE-2026-10520, the maximum-severity vulnerability stems from an OS command injection weakness. The second Sentry security flaw patched on Tuesday (tracked as CVE 2026-10523) is a critical authentication bypass that can be exploited remotely by unauthenticated attackers to create rogue administrative accounts and gain full administrative access."
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/new-max-severity-ivanti-sentry-flaw-allows-code-execution-as-root/

Critical Vulnerabilities Patched In Fortinet, Ivanti Products

"Fortinet and Ivanti on Tuesday rolled out fixes for multiple vulnerabilities in their products, including critical-severity OS command injection flaws. Fortinet published three advisories describing security defects in FortiSandbox, FortiOS, FortiProxy, and FortiPortal. The most severe of the three bugs is CVE 2026-25089

(CVSS score of 9.8), an OS command injection issue impacting FortiSandbox, FortiSandbox Cloud, and FortiSandbox PaaS WEB UI."
CERTVU recommends all users and organizations to read this Vulnerability and follow the mitigation steps to mitigate these vulnerabilities.

https://www.securityweek.com/critical-vulnerabilities-patched-in-fortinet-ivanti-products/

Oracle Mitigates PeopleSoft Zero-Day Exploited In Data Theft Attacks

"Oracle is warning about a critical PeopleSoft Suite zero-day vulnerability tracked as CVE-2026-35273 that allows unauthenticated remote code execution, with the flaw actively exploited in ShinyHunter data theft attacks. The flaw is within Oracle PeopleSoft PeopleTools and has a CVSS base score of 9.8. "This Security Alert addresses vulnerability CVE-2026-35273 in Oracle PeopleSoft PeopleTools. Oracle PeopleSoft Enterprise Applications customers may also be affected by this vulnerability," reads a new Oracle advisory."
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/oracle-mitigates-peoplesoft-zero-day-exploited-in-data-theft-attacks/

Max Severity Ivanti Sentry Vulnerability Now Exploited In Attacks

"Attackers are now targeting a recently patched maximum-severity flaw in Ivanti Sentry, enabling them to execute code with root privileges on Internet-exposed secure mobile gateways. Formerly known as MobileIron Sentry, the Ivanti Sentry security gateway appliance secures traffic between back-end corporate systems and remote mobile devices. Tracked as CVE-2026-10520, the maximum-severity vulnerability stems from an OS command injection weakness and was patched by Ivanti on Tuesday with the release of Sentry versions R10.5.2, R10.6.2, and R10.7.1."
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/max-severity-ivanti-sentry-vulnerability-now-exploited-in-attacks/

Malware

Red Hat Npm Packages Compromised To Spread a Credential-Stealing Worm

"On June 1, 2026, we detected multiple official packages from the @redhat-cloud-services scope on npm were compromised with a credential-stealing worm. In total, 96 versions across 32 packages have been compromised, cumulatively downloaded 116,991 times per week. The malware appears similar to the Mini Shai-Hulud malware that was recently open-sourced by TeamPCP. Since the tooling was made publicly available, other threat actors now have access to the same techniques and can replicate or adapt them. The packages were published via GitHub Actions OIDC, indicating the CI/CD pipeline was compromised rather than an npm token. If you have installed any affected package versions since June 1, 2026, treat all CI secrets, cloud credentials, SSH keys, and npm tokens as compromised and rotate them immediately."

https://www.aikido.dev/blog/red-hat-npm-packages-compromised-credential-stealing-worm

Game Over: WeedHack – The Rise Of Minecraft Malware-As-a-Service Campaigns

"Minecraft is a 2011 sandbox game developed and published by Mojang Studios. It is the best-selling video game in the world and has sold over 350 million copies worldwide. Its popularity has spanned over a decade due to its versatile gameplay, offering multiple game modes, including one of the most memorable Story Mode in gaming history. It allows players to create and host multiplayer servers with a variety of gameplay options and offers a wide range of custom launchers, game mods, and cheats to 2/7 choose from."

https://www.mcafee.com/blogs/other-blogs/mcafee-labs/weedhack-minecraft-malware-as-a-service-campaign-research/

Instagram Users Locked Out After Meta AI Abused To Steal Accounts

"Multiple Instagram users had their accounts hijacked after attackers convinced Meta's AI-powered support tools that they were the legitimate owners. In many cases, impacted users are unable to recover access due to the platform's use of automated assistance that involves only AI/chatbot loops and no human support agents. On Monday, multiple holders of rare and high-value accounts reported suddenly losing access to their accounts, claiming that their identities had been verified via facial scans and that they had enabled safeguards such as two-factor authentication (2FA)."

https://www.bleepingcomputer.com/news/security/instagram-users-

locked-out-after-meta-ai-abused-to-steal-accounts/

Operation FlutterBridge: MacOS Malvertising Campaign Spreads New FlutterShell Backdoor

"We are tracking an increasingly widespread malvertising campaign targeting macOS. This campaign appears to be the next stage of a previous campaign known as JSCoreRunner, which was first identified in August 2025. In recent months, the financially-motivated attackers behind these campaigns transitioned from delivering standard adware, to delivering adware with full backdoor capabilities. We designate this campaign Operation FlutterBridge, and we call the payload that it delivers FlutterShell. Built using the Flutter framework, FlutterShell infects targets with adware via malicious desktop applications. In addition to its adware functionality, the payload possesses backdoor capabilities, including shell command execution and file system manipulation."

https://unit42.paloaltonetworks.com/flutterbridge-new-fluttershell-backdoor/

NFCShare Android Malware Spreads Via Fake Banking App Updates On GitHub

"New variants of the NFCShare Android malware are being distributed as fake updates for legitimate banking apps hosted on GitHub. The malware has evolved and is now targeting customers of multiple banks and financial institutions across Europe in a phishing campaign aimed at stealing payment card data. After tricking victims with a fake verification screen to place the cards near the mobile device's 3/8 near-field communication (NFC) chip, NFCShare reads the information using Android's IsoDep interface and EMV commands."

https://www.bleepingcomputer.com/news/security/nfcshare-android-malware-spreads-via-fake-banking-app-updates-ongithub/

Fighting Spyware: An Update From WhatsApp

"WhatsApp caught and disrupted spear phishing attempts linked to NSO, a spyware firm blacklisted by the US government. Today, we're asking the court to hold NSO in contempt for violating a permanent injunction that barred them from ever targeting WhatsApp and its users. Spyware is a national security threat, which is why we are supporting a growing coalition of privacy advocates and security researchers against spyware, and donating to the Spyware Accountability Initiative."

https://about.fb.com/news/2026/06/fighting-spyware-an-update-from-whatsapp/

From Fake Amazon Security Alert To HarborWatch Agent: ClickFix Delivery Of a Custom Monitoring RAT

"Threat actors do not always need to compromise a major company to weaponize its trust; they simply need to borrow its name. In the following campaign threat, cybercriminals utilize social engineering, lookalike domains, and fake verification tactics to turn a routine security alert into a ClickFix malware delivery with the goal of convincing recipients to unknowingly infect themselves. The Cofense Phishing Defense Center has identified an Amazon-themed malware delivery campaign that abuses the ClickFix self-infection technique to deliver a custom monitoring RAT known as HarborWatch Agent. This campaign highlights a growing trend in the threat landscape where attackers are abusing trusted brands and fake verification to turn users into the mechanism of their own infection."

https://cofense.com/blog/from-fake-amazon-security-alert-to-harborwatch-agent-clickfix-delivery-of-a-custom-monitoring-rat

When "Hi, This Is IT" Comes Through Microsoft Teams

"It's Friday afternoon. The week has been busy, and everyone is wrapping up before the weekend. One of your workers receives a message (Figure 1) through Microsoft Teams from what appears to be the IT Service Provider. The message is marked as external. The worker previews the message and sees, "Hi, this is the IT Department. We see an issue with your account." The message looks routine and is in MS Teams, not email. The worker accepts the message. The conversation proceeds and the "IT technician" explains that a login anomaly was detected and asks the worker to approve a multi-factor authentication (MFA) prompt to confirm their identity. The conversation continues for a few minutes to maintain credibility, but behind the scenes the compromise is already underway."

https://unit42.paloaltonetworks.com/microsoft-teams-phishing/

AI Brands As Bait: How Threat Actors Are Using The AI Hype In Social Engineering

"As threat actors operationalize AI to accelerate attacks, they are also leveraging the wider global interest around AI itself as a social engineering lure. In recent months, Microsoft Threat Intelligence has observed a growing number of campaigns that impersonate the branding of popular AI platforms

such as ChatGPT, Microsoft Copilot, DeepSeek, and Anthropic's Claude as lures. These campaigns, which don't represent compromise of services, span phishing, malvertising, and search engine optimization (SEO)-driven attacks that ultimately lead to credential theft, financial fraud, or malware infection."

https://www.microsoft.com/en-us/security/blog/2026/06/08/ai-brands-as-bait-how-threat-actors-are-using-the-ai-hype-in-social-engineering/

Phishing Attacks Leverage TikTok, Instagram Reels

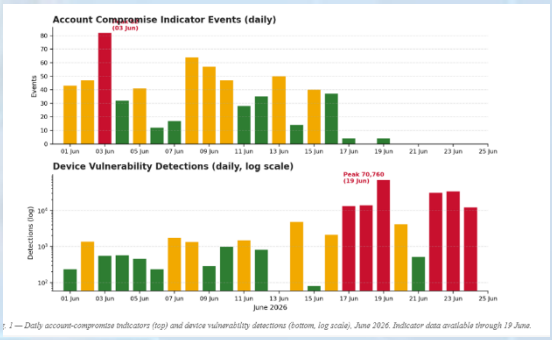
"Short-form videos on social media apps are currently being leveraged by threat actors as a phishing vector, utilizing tutorial style content with the promise of free premium software to lure victims onto malicious sites. This is an important threat to be cognizant of, as the videos can trick users into directly downloading malware. In order to best defend organizations, steps can be taken to mitigate the risks associated with these videos, both in user training and technical guardrails."

https://www.reversinglabs.com/blog/social-media-attacks-phishing

CERTVU Threat Statistics

CERTVU's Cyber Risk Index closed June at 65.8/100 (Medium risk). Thirteen days in June scored in the High-risk band (7% of days) — well above regional, industry, and organization-size peer averages of 0%. Internet-Facing Assets is the only category rated High risk this month; Devices, Accounts, and Applications sit at Medium; Cloud Assets is Low, reflecting a lack of connected cloud telemetry rather than confirmed low risk.

Threat and Vulnerability activity June



1 — Daily account-compromise indicators (top) and device vulnerability detections (bottom, log scale), June 2026. Indicator data available through 19 June.

Risk Category breakdown

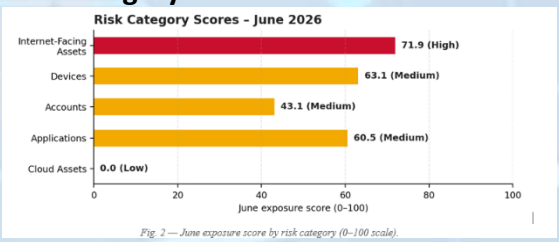


Fig. 2 — June exposure score by risk category (0–100 scale).

Key Risk Factors — June

- 21,501 detected vulnerabilities on devices; 26 confirmed cyber threats found on endpoints.
- 208 vulnerabilities and 7 unexpected exposed

© CERTVU 2026

services/ports on internet-facing hosts; 2 hosts flagged for insecure (expired/weak) TLS connections.

- 1,027 accounts with weak authentication and 953 accounts flagged as attack-surface risk (predominantly stale, inactive accounts).
- 15 account compromise events and 74 legacy-authentication log-ons recorded; 1 user account threat reached a critical attack stage.
- No risk events detected for Applications or Cloud Assets this month — a coverage gap from limited connected data sources, not a clean bill of health.

CERTVU Advisories

Advisory 152: Ubiquiti UniFi OS Path Traversal Vulnerability

CVE-2026-34910 is a critical Command Injection vulnerability affecting Ubiquiti UniFi OS devices. The vulnerability results from improper input validation, allowing a malicious actor with network access to inject and execute arbitrary operating system commands on vulnerable devices.

https://cert.gov.vu/index.php/advisories/162-advisory-152

Advisory 151: Ubiquiti UniFi OS Path Traversal Vulnerability

CVE-2026-34909 is a critical Path Traversal vulnerability affecting Ubiquiti UniFi OS devices. The flaw allows a malicious actor with network access to access files on the underlying operating system that should not be accessible through the application. These files may then be manipulated or leveraged to gain access to an underlying system account.

https://cert.gov.vu/index.php/advisories/161-advisory-151

Advisory 150: Ubiquiti UniFi OS Improper Access Control Vulnerability

CVE-2026-34908 is a critical Improper Access Control vulnerability affecting Ubiquiti UniFi OS devices. The vulnerability allows an unauthenticated attacker with network access to make unauthorized changes to the system, potentially resulting in complete compromise of the device and the networks it manages.

https://cert.gov.vu/index.php/advisories/160-advisory-150

Advisory 149: FortiBleed – Widespread Credential Exposure Targeting Fortinet Firewalls and SSL VPN Gateways

© CERTVU 2026

CERT Vanuatu advises on FortiBleed, a large-scale credential exposure campaign targeting Fortinet FortiGate Firewalls and SSL VPN gateways. Unlike a traditional software vulnerability, FortiBleed is a credential compromise campaign where attackers leverage leaked, stolen, or exposed administrator and VPN credentials to gain unauthorized access to Fortinet devices.

https://cert.gov.vu/index.php/advisories/159-advisory-149

Advisory 148: SocGholish Campaign Targeting Compromised WordPress Sites

CERT Vanuatu advises on SocGholish (also known as FakeUpdates, DEV-0206, TA569, GOLD PRELUDE, Mustard Tempest, and UNC1543) is a malware delivery framework that compromises legitimate WordPress websites and uses them to distribute malware through fake browser or software update prompts. Rather than exploiting visitors directly through a software vulnerability, attackers first compromise WordPress sites and inject malicious code that redirects users to attacker-controlled infrastructure.
According to a recent report by the Shadowserver Foundation, law enforcement and industry partners disrupted a major SocGholish operation, remediating 14,971 compromised WordPress sites and taking down 106 malicious servers and domains.

https://cert.gov.vu/index.php/advisories/158-advisory-148

Advisory 147: Widespread credential Exposure Affecting Fortinet Firewalls and VPN Gateways

CERT Vanuatu advises on a widespread malicious campaign targeting Fortinet Firewalls and VPN gateways. Unlike a single software vulnerability, this campaign primarily involves the compromise, theft, and abuse of administrative and VPN credentials, enabling attackers to gain unauthorized access to Fortinet devices and connected networks.
Attackers are leveraging exposed, weak, reused, or previously compromised credentials to authenticate to Fortinet infrastructure and potentially bypass security controls without exploiting a software vulnerability.

https://cert.gov.vu/index.php/advisories/157-advisory-147

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

Cyber month Event
October is observed as Cyber Month, a national initiative promoting safe and responsible use of digital technology and strengthening cybersecurity awareness across Vanuatu.

As part of the Cyber Up Pacific campaign, CERT Vanuatu (CERTVU) coordinates Cyber Week activities involving communities, schools, government, businesses, and other stakeholders. These activities raise awareness of cyber threats, promote good cybersecurity practices, and help people and organizations better protect their information and digital services.
Through these efforts, CERTVU contributes to a safer, stronger, and more resilient digital Vanuatu.

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.

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 Cybersecurity Agency
The Department of Communication and Digital Transformation (DCDT) is working with local stakeholders on two key initiatives: developing a **Cloud Infrastructure Roadmap** and establishing a **Cybersecurity Agency**.
The Cloud Infrastructure Roadmap will guide the adoption of cloud technologies across government, while the Cybersecurity Agency will strengthen national cybersecurity coordination, policies, and protection of digital assets.
Together, these initiatives support Vanuatu's goal of building a **secure, resilient, and digitally enabled nation**.
Capacity Building Program
CERT Vanuatu (CERTVU) continues to strengthen cybersecurity knowledge and skills through capacity-building programs

 © CERTVU 2026

in partnership with national and international organizations.

A key training program for critical infrastructure organizations was conducted from **26–30 August 2024** at the Ramada Resort by Wyndham in Port Vila, helping participants improve their cybersecurity capabilities and preparedness.

International Collaboration

CERTVU continues to strengthen international partnerships to enhance Vanuatu's cybersecurity capabilities and contribute to the wider Pacific cybersecurity community.

PACSON

Through DCDT, CERTVU actively participates in key **Pacific Cyber Security Operational Network (PACSON)** working groups, including:

- **Awareness Raising:** Promotes cybersecurity awareness through initiatives such as **CyberSmart**.
- **Community:** Supports information sharing and the development of a stronger, more resilient cyber community.
- **Capacity Building:** Strengthens cybersecurity skills through targeted training and support.

Through these partnerships, CERTVU contributes to a **safer and more secure digital environment across the Pacific**.

Incident Response

CERTVU operates a proactive **Incident Response Team** that monitors and responds to common cyber threats.

The team works to identify, mitigate, and prevent incidents while supporting individuals and organizations through monitoring, training, and awareness activities. These efforts help reduce the impact of cyber threats and strengthen cybersecurity preparedness and resilience in Vanuatu.

References

1. https://www.obsidiansecurity.com/blog/when-is-stdio-mcp-actually-a-vulnerability
2. https://www.securityweek.com/exploit-code-published-for-critical-flowise-rce-vulnerability/
3. https://www.wordfence.com/blog/2026/05/15000-wordpress-sites-affected-by-administrator-account-creation-vulnerabilityin-wp-maps-pro-wordpress-plugin/
4. https://www.bleepingcomputer.com/news/security/wp-maps-pro-bug-exploited-to-create-admin-accounts-on-wordpresssites/

5. https://www.bleepingcomputer.com/news/microsoft/critical-windows-netlogon-remote-code-execution-flaw-now-exploited-inattacks/
7. https://www.securityweek.com/critical-windows-netlogon-vulnerability-in-attackers-crosshairs/
8. https://www.helpnetsecurity.com/2026/06/01/windows-netlogon-rce-exploited-cve-2026-41089/
9. https://www.wordfence.com/blog/2026/06/unauthenticated-privilege-escalation-vulnerability-patched-in-kirki-wordpressplugin/
10. https://www.bleepingcomputer.com/news/security/critical-kirki-flaw-exploited-to-hijack-wordpress-admin-accounts/
11. https://www.bleepingcomputer.com/news/security/acer-warns-of-max-severity-zero-days-affecting-wave-7-routers/
12. https://www.wordfence.com/blog/2026/06/attackers-actively-exploiting-critical-vulnerability-in-everest-forms-pro-plugin/
13. https://www.infosecurity-magazine.com/news/everest-forms-pro-rce-actively/
14. https://www.securityweek.com/chrome-149-patches-429-vulnerabilities/
15. https://bishopfox.com/blog/popping-root-on-unifi-os-server-unauthenticated-rce-chain-detection-analysis
16. https://www.bleepingcomputer.com/news/security/critical-unifi-os-bug-lets-hackers-gain-root-without-authentication/
17. https://www.securityweek.com/sap-patches-critical-netweaver-commerce-vulnerabilities/
18. https://www.bleepingcomputer.com/news/security/sap-fixes-critical-flaws-in-netweaver-and-commerce-cloud/
19. https://www.securityweek.com/adobe-patches-123-vulnerabilities/
20. https://www.bleepingcomputer.com/news/security/new-max-severity-ivanti-sentry-flaw-allows-code-execution-as-root/
21. https://nvd.nist.gov/vuln/detail/CVE-2026-10520
22. https://www.theregister.com/patches/2026/06/10/ivanti-urges-sentry-users-to-patch-two-critical-bugs/5253428
23. https://www.helpnetsecurity.com/2026/06/10/ivanti-sentry-cve-2026-10520-cve-2026-10523/
24. https://www.securityweek.com/critical-vulnerabilities-patched-in-fortinet-ivanti-products/
25. https://thehackernews.com/2026/06/ivanti-fortinet-and-sap-release-patches.html
26. https://www.bleepingcomputer.com/news/security/oracle-mitigates-peoplesoft-zero-day-exploited-in-data-theft-attacks/
27. https://thehackernews.com/2026/06/shinyhunters-exploits-oracle-peoplesoft.html
28. https://www.securityweek.com/oracle-addresses-peoplesoft-vulnerability-amid-reports-of-zero-day-attacks/
29. https://www.helpnetsecurity.com/2026/06/11/oracle-peoplesoft-under-attack-cve-2026-35273/

30. https://www.bleepingcomputer.com/news/security/max-severity-ivanti-sentry-vulnerability-now-exploited-in-attacks/
31. https://www.darkreading.com/vulnerabilities-threats/max-severity-ivanti-sentry-flaw-exploited-24-hours
32. https://securityaffairs.com/193530/uncategorized/cve-2026-10520-exploited-ivanti-sentry-gateways-compromised-shortlyafter-patch-release.html
33. https://www.securityweek.com/splunk-palo-alto-networks-patch-severe-vulnerabilities/
34. https://www.aikido.dev/blog/red-hat-npm-packages-compromised-credential-stealing-worm
35. https://www.ox.security/blog/new-npm-supply-chain-attack-redhat-cloud-services-compromised/
37.
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_whn_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://cert.gov.vu/index.php/advisories?start=42
44. https://www.facebook.com/CERTVU

© CERTVU 2026