MONTHLY BULLETIN

Cert Vanuatu Security Bulletin

May
2025

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

CONTACTS

QUOTE OF THE MONTH!

"If you think technology can solve your security problems, then you don't understand the problems and you don't understand the technology."
— Bruce Schneier

OVERVIEW

CERT Vanuatu, operating under the Department of Communication and Digital Transformation, is pleased to release our latest monthly security bulletin. This edition covers key vulnerabilities and active exploits identified throughout May 2025 across various computer networks, systems, and applications.

We trust this bulletin will serve as a valuable resource in strengthening your organization's cybersecurity posture.

CERT VANUATU EFFORTS

CERT Vanuatu (CERT-VU) plays a vital role in strengthening Vanuatu's cybersecurity efforts. Through close collaboration with a wide range of stakeholders, CERT-VU addresses cybersecurity challenges at multiple levels, with the goal of building a community that is both cyber-aware and resilient against digital threats.

CERTVU OPERATIONS

CYBER SECURITY AWARENESS PROGRAM

As part of our ongoing awareness program, we are actively engaged in several initiatives. A key component of our outreach is partnering with Platform Radio Vanuatu's morning shows, where we share informative and engaging discussions on ICT to help educate and empower the public.

Family I ready (FIR)

CERT Vanuatu (CERTVU) is collaborating with World Vision Vanuatu on the "Famili i Redi" Project to raise awareness about safety and security for RSE and SWP seasonal workers. The initiative aims to ensure these workers are well-informed about protecting themselves and their families during extended periods of separation, which can span several months or even years. The project also encourages the use of ICT and the Internet as vital tools for staying connected with loved ones in their home villages and islands.

ICT Talks at VTBC

VBTC is hosting a weekly Cybersecurity Awareness program every Friday from 8 to 9 AM, featuring CERT Vanuatu (CERTVU). Each session delivers important cybersecurity messages for both individuals and entities, covering various topics such as online safety, data protection, phishing scams, and cyber threats. The program aims to educate the public and organizations on best practices to stay secure in the digital world.

CAPACITY BUILDING

CERT Vanuatu (CERT-VU) has remained committed to strengthening its international partnerships over the years, aiming to elevate its standing in the global cybersecurity arena. By actively collaborating with cybersecurity organizations across the Pacific and beyond, CERT-VU consistently exchanges knowledge and best practices to improve its capabilities.

Through continued involvement in joint projects and information-sharing forums, CERT-VU plays a key role in promoting lasting international cooperation, helping to ensure a safer digital environment for both Vanuatu and the global community.

CERTVU OPERATIONS

INTERNATIONAL COLLABORATION

CERT Vanuatu (CERT-VU) continues to strengthen its international partnerships, with a clear focus on enhancing its role in the global cybersecurity landscape. By actively engaging with cybersecurity organizations across the Pacific and beyond, CERT-VU regularly shares knowledge and best practices to boost its operational effectiveness.

Through sustained participation in collaborative projects and information-sharing platforms, CERT-VU contributes significantly to fostering long-term international cooperation—supporting a safer and more resilient digital environment for Vanuatu and the wider global community.

INCIDENT RESPONSE

CERTVU maintains a proactive incident response team dedicated to managing daily cyber threats. This team is essential in defending against a broad spectrum of sophisticated attacks, including phishing, ransomware, malware, and social engineering tactics.

Phishing remains the most prevalent and impactful threat, representing nearly 50% of all incidents handled by the team. This underscores both the widespread nature of phishing campaigns and the growing emphasis cybercriminals place on exploiting human vulnerabilities to breach security measures.

EVENT

DIGITAL WEEK-VANUATU

Since its inception in 2011, National ICT Days have grown into one of Vanuatu's most recognized and anticipated annual events. In 2021, we proudly celebrated a decade of its success. Over the years, we've redefined the standard for event planning and coordination—setting a benchmark that continues to stand unmatched. As the event has evolved, we remain proud to lead the way in shaping how major events are delivered in Vanuatu.

In 2025, for the first time, National ICT Days merged with two other major national events—Consumer Rights Day and the E-Commerce Symposium—forming a unified and more impactful initiative known as Digital Week. This milestone week brought together key themes of digital innovation, consumer empowerment, and economic growth under one banner.

Digital Week 2025 took place from 13 to 16 May 2025 at Unity Park in Luganville, Santo, under the theme: "Innovate Today, Sustain Tomorrow." The event was a great success, reaching a wide audience across Santo and Luganville, including local communities and schools. It fostered strong engagement, promoted digital awareness, and encouraged participation in conversations around technology, consumer rights, and e-commerce.

CYBERSECURITY BOOTH CAMP

As a side Event of the Digital week, this year the Cybersecurity Booth Camp has convened as well in Santo. it included the senior schools in Santo. The students had the opportunity to participate in a Cybersecurity Boot Camp, an intensive training session led by CERTVU. This hands-on experience covers key areas such as ethical hacking, threat detection, digital forensics, and cyber incident response. The boot camp enhances students' practical skills, preparing them to tackle real-world cybersecurity challenges and strengthen digital defenses in Vanuatu and beyond.

VULNERABILITIES AND ACTIVE EXPLOITS

1.RECENTLY DISCLOSED SURETRIGGERS CRITICAL PRIVILEGE ESCALATION VULNERABILITY UNDER ACTIVE EXPLOITATION

"On May 2nd, 2025 the Wordfence Threat Intelligence team added a new critical vulnerability to the Wordfence Intelligence vulnerability database in the OttoKit: All-in-One Automation Platform (Formerly SureTriggers) plugin publicly disclosed by a third-party CNA on April 30th, 2025. This vulnerability makes it possible for unauthenticated attackers to gain administrative level access to vulnerable sites, where the site has never used an application password nor connected to OttoKit/SureTriggers using an application password, or by authenticated attackers with a valid application password."

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

https://www.wordfence.com/blog/2025/05/recently-disclosed-suretriggers-critical-privilege-escalation-vulnerability-under-active-exploitation/

2.CISCO PATCHES CVE-2025-20188 (10.0 CVSS) IN IOS XE THAT ENABLES ROOT EXPLOITS VIA JWT

"Cisco has released software fixes to address a maximum-severity security flaw in its IOS XE Wireless Controller that could enable an unauthenticated, remote attacker to upload arbitrary files to a susceptible system. The vulnerability, tracked as CVE-2025-20188, has been rated 10.0 on the CVSS scoring system. "This vulnerability is due to the presence of a hard-coded JSON Web Token (JWT) on an affected system," the company said in a Wednesday advisory."

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

https://thehackernews.com/2025/05/cisco-patches-cve-2025-20188-100-cvss.html

3.MICROSOFT MAY 2025 PATCH TUESDAY FIXES 5 EXPLOITED ZERO-DAYS, 72 FLAWS

"Today is Microsoft's May 2025 Patch Tuesday, which includes security updates for 72 flaws, including 1/9 five actively exploited and two publicly disclosed zero-day vulnerabilities. This Patch Tuesday also fixes six "Critical" vulnerabilities, five being remote code execution vulnerabilities and another an information disclosure bug."

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

https://www.tripwire.com/state-of-security/may-2025-patch-tuesday-analysis

VULNERABILITIES AND ACTIVE EXPLOITS

4.SAP PATCHES SECOND ZERO-DAY FLAW EXPLOITED IN RECENT ATTACKS

"SAP has released patches to address a second vulnerability exploited in recent attacks targeting SAP NetWeaver servers as a zero-day. The company issued security updates for this security flaw (CVE□2025-42999) on Monday, May 12, saying it was discovered while investigating zero-day attacks involving another unauthenticated file upload flaw (tracked as CVE-2025-31324) in SAP NetWeaver Visual Composer that was fixed in April. "SAP is aware of and has been addressing vulnerabilities in SAP NETWEAVER Visual Composer," a SAP spokesperson told BleepingComputer. "We ask all customers using SAP NETWEAVER to install these patches to protect themselves. The Security Notes can be found here: 3594142 & 3604119."
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/sap-patches-second-zero-day-flaw-exploited-in-recent-attacks/

5.FORTINET FIXES CRITICAL ZERO-DAY EXPLOITED IN FORTIVOICE ATTACKS

"Fortinet released security updates to patch a critical remote code execution vulnerability exploited as a zero-day in attacks targeting FortiVoice enterprise phone systems. The security flaw is a stack-based overflow vulnerability tracked as CVE-2025-32756 that also impacts FortiMail, FortiNDR, FortiRecorder, and FortiCamera. As the company explains in a security advisory issued on Tuesday, successful exploitation can allow remote unauthenticated attackers to execute arbitrary code or commands via maliciously crafted HTTP requests."
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/fortinet-fixes-critical-zero-day-exploited-in-fortivoice-attacks/

VULNERABILITIES AND ACTIVE EXPLOITS

6.SAMSUNG PATCHES CVE-2025-4632 USED TO DEPLOY MIRAI BOTNET VIA MAGICINFO 9 EXPLOIT

"Samsung has released software updates to address a critical security flaw in MagicINFO 9 Server that has been actively exploited in the wild. The vulnerability, tracked as CVE-2025-4632 (CVSS score: 9.8), has been described as a path traversal flaw. "Improper limitation of a pathname to a restricted directory vulnerability in Samsung MagicINFO 9 Server version before 21.1052 allows attackers to write arbitrary files as system authority," according to an advisory for the flaw."

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

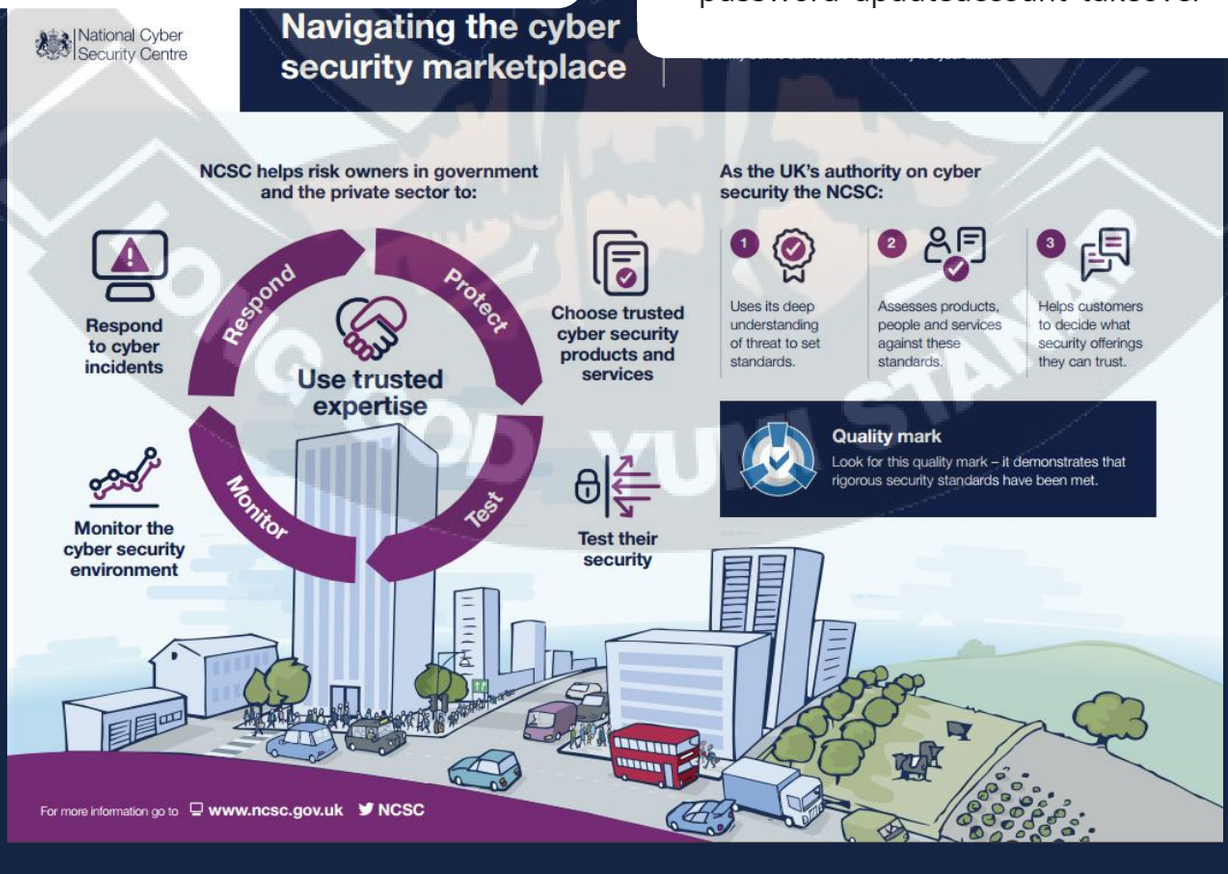
https://thehackernews.com/2025/05/samsung-patches-cve-2025-4632-used-to.html

7.MOTORS <= 5.6.67 - UNAUTHENTICATED PRIVILEGE ESCALATION VIA PASSWORD UPDATE/ACCOUNT TAKEOVER

"The Motors theme for WordPress is vulnerable to privilege escalation via account takeover in all versions up to, and including, 5.6.67. This is due to the theme not properly validating a user's identity prior to updating their password. This makes it possible for unauthenticated attackers to change arbitrary user passwords, including those of administrators, and leverage that to gain access to their account."

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

https://www.wordfence.com/threat-intel/vulnerabilities/wordpress-themes/motors/motors-5667-unauthenticated-privilege-escalation-via-password-updateaccount-takeover



VULNERABILITIES AND ACTIVE EXPLOITS

8.CVE-2025-47949 REVEALS FLAW IN SAMLIFY THAT OPENS DOOR TO SAML SINGLE 1/9 SIGN-ON BYPASS

"A new critical vulnerability popped up concerning samlify, a widely adopted Node.js library for implementing SAML 2.0 Single Sign-On. So, what exactly do you need to know about this? This post will break down the flaw, its potential impact on applications using samlify, and most importantly, guide you on how to secure your systems. Understanding this vulnerability is crucial for anyone involved in managing SAML-based authentication."
CERTVU recommends all users and organizations to read this advisory and follow the mitigation steps to mitigate these vulnerabilities.

https://www.endorlabs.com/learn/cve-2025-47949-reveals-flaw-in-samlify-that-opens-door-to-saml-single-sign-on-bypass

9.UNPATCHED CRITICAL BUGS IN VERSA CONCERTO LEAD TO AUTH BYPASS, RCE

"Critical vulnerabilities in Versa Concerto that are still unpatched could allow remote attackers to bypass authentication and execute arbitrary code on affected systems. Three security issues, two of them critical, were publicly disclosed by researchers at the vulnerability management firm ProjectDiscovery after reporting them to the vendor and receiving no confirmation of the bugs being addressed. Versa Concerto is the centralized management and orchestration platform for Versa Networks' SD-WAN and SASE (Secure Access Service Edge) solutions."
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/unpatched-critical-bugs-in-versa-concerto-lead-to-auth-bypass-rce/

10.UNPATCHED CRITICAL VULNERABILITY IN TI WOOCOMMERCE WISHLIST PLUGIN

"This blog post is about an unauthenticated arbitrary file upload in the TI WooCommerce Wishlist plugin. If you're a TI WooCommerce Wishlist user, deactivate and delete the plugin since there is no patched version available. All paid Patchstack users are protected from this vulnerability. Sign up for the free Community account first, to scan for vulnerabilities and apply protection for only $5 / site per month with Patchstack. For plugin developers, we have security audit services and Enterprise API for hosting companies."
CERTVU recommends all users and organizations to read this advisory and follow the mitigation steps to mitigate these vulnerabilities.

https://patchstack.com/articles/unpatched-critical-vulnerability-in-ti-woocommerce-wishlist-plugin/

MALWARE

1.IVANTI EPMM RCE VULNERABILITY CHAIN EXPLOITED IN THE WIL

"On March 13th, 2025, Ivanti disclosed that Endpoint Manager Mobile (EPMM) is affected by a vulnerability chain combining an authentication bypass (CVE-2025-4427) and a post-authentication remote code execution vulnerability (CVE-2025-4428). These flaws, which stem from unsafe use of Java Expression Language in error messages and misconfigured routing, can be exploited together to achieve unauthenticated RCE. Therefore, while neither of these vulnerabilities have been assigned critical severity (their CVSS scores are 5.3 and 7.2, respectively), in combination they should certainly be treated as critical. Ivanti has confirmed limited exploitation in-the-wild of these vulnerabilities as 0- days prior to their disclosure, and Wiz can now confirm ongoing exploitation in-the-wild of these vulnerabilities."

https://www.wiz.io/blog/ivanti-epmm-rce-vulnerability-chain-cve-2025-4427-cve-2025-4428

2.DISRUPTING LUMMA STEALER: MICROSOFT LEADS GLOBAL ACTION AGAINST FAVORED CYBERCRIME TOOL

"Microsoft's Digital Crimes Unit (DCU) and international partners are disrupting the leading tool used to indiscriminately steal sensitive personal and organizational information to facilitate cybercrime. On Tuesday, May 13, Microsoft's DCU filed a legal action against Lumma Stealer ("Lumma"), which is the favored info-stealing malware used by hundreds of cyber threat actors. Lumma steals passwords, credit cards, bank accounts, and cryptocurrency wallets and has enabled criminals to hold schools for ransom, empty bank accounts, and disrupt critical services."

https://blogs.microsoft.com/on-the-issues/2025/05/21/microsoft-leads-global-action-against-favored-cybercrime-tool/

3.HACKER SELLING CRITICAL ROUNDCUBE WEBMAIL EXPLOIT AS TECH INFO DISCLOSED

"Hackers are likely starting to exploit CVE-2025-49113, a critical vulnerability in the widely used Roundcube open-source webmail application that allows remote execution. The security issue has been present in Roundcube for over a decade and impacts versions of Roundcube webmail 1.1.0 through 1.6.10. It received a patch on June 1st. It took attackers just a couple of days to reverse engineer the fix, weaponize the vulnerability, and start selling a working exploit on at least one hacker forum."

https://www.bleepingcomputer.com/news/security/hacker-selling-critical-roundcube-webmail-exploit-as-tech-info-disclosed/

REFERENCES

1.https://www.wordfence.com/blog/2025/05/recently-disclosed-suretriggers-critical-privilege-escalation-vulnerability-under-active-exploitation/
2.https://www.securityweek.com/second-ottokit-vulnerability-exploited-to-hack-wordpress-sites/
3.https://www.bleepingcomputer.com/news/security/hackers-exploit-ottokit-wordpress-plugin-flaw-to-add-admin-accounts/>
4.https://thehackernews.com/2025/05/cisco-patches-cve-2025-20188-100-cvss.html
5.https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-wlc-file-uplpd-rHZG9UfC
6.https://www.bleepingcomputer.com/news/security/cisco-fixes-max-severity-ios-xe-flaw-letting-attackers-hijack-devices/
7.https://www.securityweek.com/cisco-patches-35-vulnerabilities-across-several-products/
8.https://securityaffairs.com/177609/security/cisco-fixed-a-critical-flaw-in-its-ios-xe-wireless-controller.html
9.https://www.bleepingcomputer.com/news/microsoft/microsoft-may-2025-patch-tuesday-fixes-5-exploited-zero-days-72-flaws/
10.https://blog.talosintelligence.com/microsoft-patch-tuesday-for-may-2025-snort-rules-and-prominent-vulnerabilities/
11.https://blog.talosintelligence.com/microsoft-patch-tuesday-for-may-2025-snort-rules-and-prominent-vulnerabilities/
12.https://www.darkreading.com/vulnerabilities-threats/windows-zero-day-bug-exploited-browser-rce
13.https://www.securityweek.com/zero-day-attacks-highlight-another-busy-microsoft-patch-tuesday/
14.https://www.helpnetsecurity.com/2025/05/13/patch-tuesday-microsoft-fixes-5-actively-exploited-zero-days/
15.https://cyberscoop.com/microsoft-patch-tuesday-may-2025/
16.https://www.helpnetsecurity.com/2025/05/13/patch-tuesday-microsoft-fixes-5-actively-exploited-zero-days/
17.https://www.theregister.com/2025/05/14/patch_tuesday_may/
18.https://www.bleepingcomputer.com/news/security/sap-patches-second-zero-day-flaw-exploited-in-recent-attacks/
19.https://support.sap.com/en/my-support/knowledge-base/security-notes-news/may-2025.html
20.https://www.securityweek.com/sap-patches-another-critical-netweaver-vulnerability/
21.https://www.bleepingcomputer.com/news/security/fortinet-fixes-critical-zero-day-exploited-in-fortivoice-attacks/
22.https://fortiguard.fortinet.com/psirt/FG-IR-25-254
23.https://www.helpnetsecurity.com/2025/05/13/zero-day-exploited-to-compromise-fortinet-fortivoice-systems-cve-2025-32756/
24.https://thehackernews.com/2025/05/samsung-patches-cve-2025-4632-used-to.html
25.https://www.cve.org/CVERecord?id=CVE-2025-4632
26.https://www.huntress.com/blog/post-exploitation-activities-observed-from-samsung-magicinfo-9-server-flaw
27.https://www.wordfence.com/threat-intel/vulnerabilities/wordpress-themes/motors/motors-5667-unauthenticated-privilege-escalation-via-password-updateaccount-takeover
28.https://www.bleepingcomputer.com/news/security/premium-wordpress-motors-theme-vulnerable-to-admin-takeover-attacks/
29.https://www.endorlabs.com/learn/cve-2025-47949-reveals-flaw-in-samlify-that-opens-door-to-saml-single-sign-on-bypass
30.https://nvd.nist.gov/vuln/detail/CVE-2025-47949
31.https://www.bleepingcomputer.com/news/security/critical-samlify-sso-flaw-lets-attackers-log-in-as-admin/
32.https://www.bleepingcomputer.com/news/security/unpatched-critical-bugs-in-versa-concerto-lead-to-auth-bypass-rce/
33.https://www.infosecurity-magazine.com/news/critical-zerodays-versa-networks/
34.https://www.infosecurity-magazine.com/news/critical-zerodays-versa-networks/
35.https://patchstack.com/articles/unpatched-critical-vulnerability-in-ti-woocommerce-wishlist-plugin/
36.https://thehackernews.com/2025/05/over-100000-wordpress-sites-at-risk.html
37.https://www.wiz.io/blog/ivanti-epmm-rce-vulnerability-chain-cve-2025-4427-cve-2025-4428
38.https://www.theregister.com/2025/05/21/ivanti_rce_attacks_ongoing/
39.https://blogs.microsoft.com/on-the-issues/2025/05/21/microsoft-leads-global-action-against-favored-cybercrime-tool/
40.https://www.securityweek.com/microsoft-sinkholes-domains-disrupts-notorious-lumma-stealer-malware-operation/
41.https://www.bleepingcomputer.com/news/security/lumma-infostealer-malware-operation-disrupted-2-300-domains-seized/
42.https://www.bleepingcomputer.com/news/security/hacker-selling-critical-roundcube-webmail-exploit-as-tech-info-disclosed/