CertVu

MONTHLY BULLETIN

DCDT

Cert Vanuatu Security Bulletin

March
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!

"Cybersecurity is not just about technology; it's about people, processes, and vigilance. The weakest link in security is often human error,stay aware, stay prepared." CERTVU

OVERVIEW

CERT Vanuatu, under the Department of Communication and Digital Transformation, is excited to share our latest monthly security bulletin. In this issue, we highlight the vulnerabilities and ongoing exploits identified during 2025 in various Computer network, systems and applications.
We hope this bulletin proves to be a useful resource for enhancing your organization's security preparedness.

CERT VANUATU EFFORTS

CERT Vanuatu (CERT-VU) is instrumental in bolstering Vanuatu's cybersecurity initiatives. By working closely with diverse stakeholders, CERT-VU tackles cybersecurity challenges on various levels, aiming to create a community that is both well-informed about cybersecurity and resilient to cyber threats.

CERTVU OPERATIONS

CYBER SECURITY AWARENESS PROGRAM

We are currently involved in several initiatives as part of our ongoing awareness program. One of our key outreach efforts is through Platform Radio Vanuatu's morning shows, where we deliver engaging ICT discussions to educate and inform the public.

Family I ready (FIR)

CERT Vanuatu (CERTVU) is partnering with World Vision Vanuatu on the "Famili i Redi" Project to provide proper safety and security awareness for RSE and SWP seasonal workers. The goal is to ensure they are informed about their own safety and security, as well as that of their families, during long periods of separation, which can last for several months or even years. The project also promotes the use of ICT and the Internet as tools to stay in touch with their families back in their 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.

UP PACIFIC
UPGRADE
UPDATE
Famili i Redi
Labor Mobility: Not an Individual Journey, but a Family Journey

CERTVU OPERATIONS

INTERNATIONAL COLLABORATION

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.

INCIDENT RESPONSE

CERTVU operates a proactive incident response team that focuses on handling common cyber threats on a daily basis.

This team plays a crucial role in protecting against a wide range of advanced cyberattacks, such as phishing, ransomware, malware, and social engineering techniques. Phishing, in particular, stands out as the most frequent and effective threat, accounting for nearly 50% of all incidents the team addresses. This highlights not only the widespread nature of phishing attempts but also the increasing focus cybercriminals place on exploiting human weaknesses to compromise security defenses.

You can find information and news about almost anything on the internet.

But what's true ... and what isn't?

Misinformation, disinformation and fake news are all commonplace on social media, texts and emails, websites, documents and word of mouth, so it's important that you can tell the difference between what's true and what isn't.

Start by searching 'fake news' on your Get Safe Online website.

#GSOTrueOrFalse

#GetTheWorldSafeOnline

www.getsafeonline.org.vu

GET SAFE ONLINE
UK International Development
Partnership | Progress | Prosperity
CertVu

CERTVU OPERATIONS

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.

Diploma in Information & Communication Technology
National University of Vanuatu

The Cyber Emergency Response Team of Vanuatu (CERTVU) is a lecturer for this diploma, providing students with real-world cybersecurity expertise. This Diploma in ICT equips students with essential skills in computer systems, networking, software development, and cybersecurity, preparing them for careers such as Network Technician, IT Support Specialist, Full Stack Developer, and Database Administrator. Graduates are job-ready for both local and international IT markets, with opportunities to earn certifications like CCNA or CompTIA. Applicants must have completed secondary school or Certificate IV, with minimum 60% in Mathematics and ICT, pass entry tests, and demonstrate English proficiency.

UPCOMING EVENT

NATIONAL ICT DAYS

Since 2011, National ICT Days have grown and become well known throughout the country as the event of the year. In 2021, Vanuatu has celebrated 10 years of the event existence. We revolutionized the standard of organizing and coordinating events, which will always be compared to none. National ICT Days will evolve, and we are proud to be the event that sets the benchmark for event organizing and coordination in Vanuatu.

2025 Event

The 2025 National ICT will convene at Unity Park, Luganville, Santo from 12 May to 16 May 2025.

CYBERSECURITY BOOTH CAMP

As a side Event of the National ICT Days, this year the Cybersecurity Booth Camp will convene as well in Santo. it will include the senior schools in Santo. The students have 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.ELASTIC RELEASES URGENT FIX FOR CRITICAL KIBANA VULNERABILITY ENABLING REMOTE CODE EXECUTION

"Elastic has rolled out security updates to address a critical security flaw impacting the Kibana data visualization dashboard software for Elasticsearch that could result in arbitrary code execution. The vulnerability, tracked as CVE-2025-25012, carries a CVSS score of 9.9 out of a maximum of 10.0. It has been described as a case of prototype pollution. "Prototype pollution in Kibana leads to arbitrary code execution via a crafted file upload and specifically crafted HTTP requests," the company said in an advisory released Wednesday."

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

https://thehackernews.com/2025/03/elastic-releases-urgent-fix-for.html>

2.MICROSOFT MARCH 2025 PATCH TUESDAY FIXES 7 ZERO-DAYS, 57 FLAWS

"Today is Microsoft's March 2025 Patch Tuesday, which includes security updates for 57 flaws, including six actively exploited zero-day vulnerabilities. This Patch Tuesday also fixes six "Critical" vulnerabilities, all remote code execution vulnerabilities."

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

https://www.bleepingcomputer.com/news/microsoft/microsoft-march-2025-patch-tuesday-fixes-7-zero-days-57-flaws/

3.CRITICAL LFI TO RCE VULNERABILITY IN WP GHOST PLUGIN AFFECTING 200K+ SITES

"This blog post is about the WP Ghost plugin vulnerability. If you're a WP Ghost user, please update the plugin to at least version 5.4.02."

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

https://patchstack.com/articles/critical-lfi-to-rce-vulnerability-in-wp-ghost-plugin-affecting-200k-sites/

VULNERABILITIES AND ACTIVE EXPLOITS

4.IBM SCORES PERFECT 10 … VULNERABILITY IN MISSION-CRITICAL OS AIX

"IBM "strongly recommends" customers running its Advanced Interactive eXecutive (AIX) operating system apply patches after disclosing two critical vulnerabilities, one of which has a perfect 10 severity score. The two vulnerabilities, CVE-2024-56346 (10) and CVE-2024-56347 (9.6), both allow remote attackers to execute arbitrary commands. IBM's security bulletin states that both are caused by improper process controls (CWE-114). IBM has never specified the number of clients on AIX, but third‑party sources suggest around 9,000 organizations use the OS, which is generally deployed in critical applications powering high-value industries."
CERTVU recommends all users and organizations to read this advisory and follow the mitigation steps to mitigate these vulnerabilities.

https://www.theregister.com/2025/03/19/ibm_aix_critical_vulnerabilities/

5.BY EXECUTIVE ORDER, WE ARE BANNING BLACKLISTS - DOMAIN-LEVEL RCE IN VEEAM BACKUP & REPLICATION (CVE-2025-23120)

"It's us again! Once again, we hear the collective groans - but we're back and with yet another merciless pwnage of an inspired and clearly comprehensive RCE solution - no, wait, it's another vuln in yet another backup and replication solution.. While we would enjoy a world in which we could be a little merciful - today we'll explore the painful world of blacklist-based security mechanisms. You can treat this post as a natural continuation of our CVE-2024-40711 writeup, which was written by fellow watchTowr Labs team member Sina Kheirkhah (@SinSinology)."
CERTVU recommends all users and organizations to read this advisory and follow the mitigation steps to mitigate these vulnerabilities.

https://labs.watchtowr.com/by-executive-order-we-are-banning-blacklists-domain-level-rce-in-veeam-backup-replication-cve-2025-23120/

ADVISORY 81: CISCO SMALL BUSINESS ROUTER VULNERABILITY CVE-2023-20118

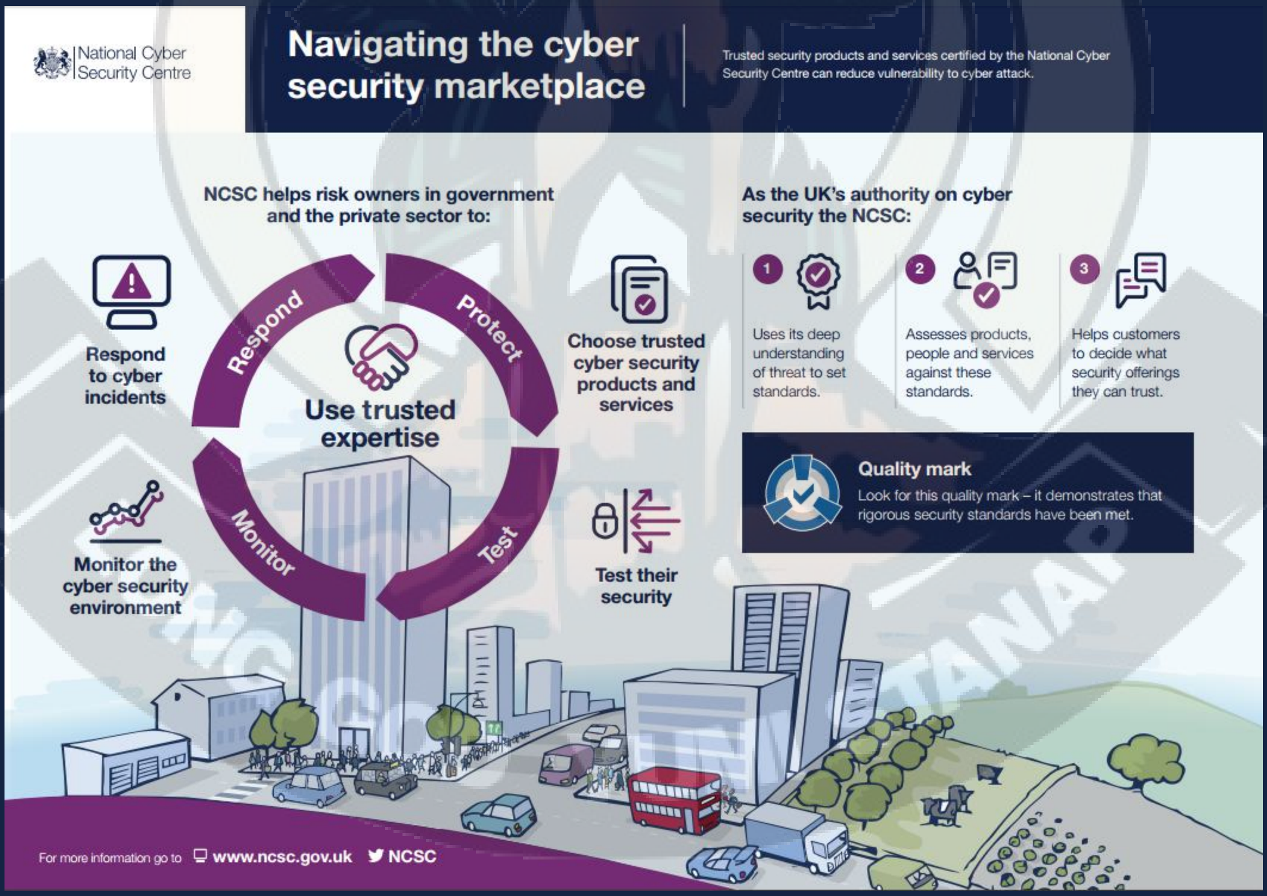
Multiple Cisco Small Business TV Series Routers contains a command injection vulnerability in the web-based management interface.

https://cert.gov.vu/index.php/services/online-advisories-alerts/253-advisory-81

ADVISORY 82: CISA ADDS FOUR KNOWN EXPLOITED VULNERABILITIES

CISA has released four new vulnerabilities based on evidence of active exploitation.
CVE-2024-50302 – Linux Kernel Use of Uninitialized Resource Vulnerability
CVE-2025-22225 – VMware ESXi Arbitrary Write Vulnerability
CVE-2025-22224 – Vmware ESXi and Workstation TOCTOU Race Condition Vulnerability
CVE-2025-22226 – Vmware ESXi, Workstation, and Fusion Information Disclosure Vulnerability
These types of vulnerabilities are frequent attack vectors for malicious cyber actors and pose significant risks to the federal enterprise.

https://cert.gov.vu/index.php/services/online-advisories-alerts/236-advisory-82



National Cyber Security Centre

Navigating the cyber security marketplace

Trusted security products and services certified by the National Cyber Security Centre can reduce vulnerability to cyber attack.

NCSC helps risk owners in government and the private sector to:

Respond to cyber incidents
Respond
Protect
Use trusted expertise
Monitor
Test
Choose trusted cyber security products and services
Monitor the cyber security environment
Test their security

As the UK's authority on cyber security the NCSC:

1 Uses its deep understanding of threat to set standards.

2 Assesses products, people and services against these standards.

3 Helps customers to decide what security offerings they can trust.

Quality mark

Look for this quality mark – it demonstrates that rigorous security standards have been met.

For more information go to www.ncsc.gov.uk NCSC

1.GREYNOISE DETECTS MASS EXPLOITATION OF CRITICAL PHP-CGI VULNERABILITY (CVE-2024-4577), SIGNALING BROAD CAMPAIGN

"Cisco Talos recently uncovered a sophisticated attack campaign targeting Japanese organizations through CVE-2024-4577, a critical PHP-CGI remote code execution flaw with 79 exploits available. While Talos focused on victimology and attacker tradecraft, GreyNoise telemetry reveals a far wider exploitation pattern demanding immediate action from defenders globally."

https://www.greynoise.io/blog/mass-exploitation-critical-php-cgi-vulnerability-cve-2024-457

2.HARDEN-RUNNER DETECTION: TJ-ACTIONS/CHANGED-FILES ACTION IS COMPROMISED

"We are actively investigating a critical security incident involving the tj-actions/changed-files GitHub Action. While our investigation is ongoing, we want to alert users so they can take immediate corrective actions. We will keep this post updated as we learn more. StepSecurity Harden-Runner detected this issue through anomaly detection when an unexpected endpoint appeared in the network traffic. Based on our analysis, the incident started around 9:00 AM March 14th, 2025 Pacific Time (PT) / 4:00 PM March 14th, 2025 UTC."

https://www.infosecurity-magazine.com/news/tjactions-supply-chain-attack/

3.NEW GITHUB ACTION SUPPLY CHAIN ATTACK: REVIEWDOG/ACTION-SETUP

"A supply chain attack on the popular GitHub Action tj-actions/changed-files caused many repositories to leak their secrets over the weekend. Wiz Research has discovered an additional supply chain attack on reviewdog/actions-setup@v1, that may have contributed to the compromise of tj-actions/changed‑files. At this point we believe this is a chain of supply chain attacks eventually leading to a specific high‑value target."

https://www.wiz.io/blog/new-github-action-supply-chain-attack-reviewdog-action-setup

4.TECHNICAL ADVISORY: MASS EXPLOITATION OF CVE-2024-4577

"Bitdefender Labs is tracking new campaigns as threat actors exploit a vulnerability we first highlighted in June 2024. Bitdefender issued a critical security advisory regarding CVE-2024-4577, a severe argument injection vulnerability in PHP affecting Windows-based systems running in CGI mode. This flaw allowed remote attackers to execute arbitrary code by manipulating character encoding conversions."

https://www.bitdefender.com/en-us/blog/businessinsights/technical-advisory-update-mass-exploitation-cve-2024-4577

REFERENCES

1.https://thehackernews.com/2025/03/elastic-releases-urgent-fix-for.html>
2.https://discuss.elastic.co/t/kibana-8-17-3-security-update-esa-2025-06/375441
3.https://securityaffairs.com/174999/security/elastic-kibana-critical-flaw.html
4.https://www.bleepingcomputer.com/news/microsoft/microsoft-march-2025-patch-tuesday-fixes-7-zero-days-57-flaws/
5.https://www.darkreading.com/application-security/whopping-number-microsoft-zero-days-under-attack
6.https://blog.talosintelligence.com/march-patch-tuesday-release/
7.https://www.tripwire.com/state-of-security/march-2025-patch-tuesday-analysis
8.https://cyberscoop.com/microsoft-patch-tuesday-march-2025/
9.https://www.securityweek.com/patch-tuesday-microsoft-patches-57-flaws-flags-six-active-zero-days/
10.https://www.theregister.com/2025/03/12/patch_tuesday/
11.https://www.theregister.com/2025/03/19/ibm_aix_critical_vulnerabilities/
12.https://labs.watchtowr.com/by-executive-order-we-are-banning-blacklists-domain-level-rce-in-veeam-backup-replication-cve-2025-23120/
13.https://www.veeam.com/kb4724
14.https://www.bleepingcomputer.com/news/security/veeam-rce-bug-lets-domain-users-hack-backup-servers-patch-now/
15.https://thehackernews.com/2025/03/veeam-and-ibm-release-patches-for-high.html
16.https://www.bankinfosecurity.com/veeam-update-patches-critical-backup-software-vulnerability-a-27782
17.https://www.securityweek.com/veeam-patches-critical-vulnerability-in-backup-replication/
18.https://securityaffairs.com/175674/slider/veeam-critical-backup-replication-vulnerability.html
19.https://www.helpnetsecurity.com/2025/03/20/critical-veeam-backup-replication-rce-vulnerability-cve-2025-23120/
20.https://www.theregister.com/2025/03/20/infoseccers_criticize_veeam_over_critical/
21.https://patchstack.com/articles/critical-lfi-to-rce-vulnerability-in-wp-ghost-plugin-affecting-200k-sites/
22.https://cert.gov.vu/index.php/services/online-advisories-alerts/236-advisory-81
23.https://cert.gov.vu/index.php/services/online-advisories-alerts/236-advisory-82
24.https://www.greynoise.io/blog/mass-exploitation-critical-php-cgi-vulnerability-cve-2024-457
25.https://www.securityweek.com/mass-exploitation-of-critical-php-vulnerability-begins/
26.https://securityaffairs.com/175198/hacking/experts-warn-of-mass-exploitation-of-critical-php-flaw-cve-2024-4577.html
27.https://www.stepsecurity.io/blog/harden-runner-detection-tj-actions-changed-files-action-is-compromised
28.https://thehackernews.com/2025/03/github-action-compromise-puts-cicd.html
29.https://www.bleepingcomputer.com/news/security/supply-chain-attack-on-popular-github-action-exposes-ci-cd-secrets/
30.https://therecord.media/github-restores-code-malicious-tj-actions-changes
31.https://www.bankinfosecurity.com/supply-chain-attack-targets-github-repositories-secrets-a-27737
32.https://www.securityweek.com/popular-github-action-targeted-in-supply-chain-attack/
33.https://hackread.com/malicious-code-in-tj-actions-changed-files-github-repos/
34.https://www.infosecurity-magazine.com/news/tjactions-supply-chain-attack/
35.https://www.infosecurity-magazine.com/news/tjactions-supply-chain-attack/
36.https://www.wiz.io/blog/new-github-action-supply-chain-attack-reviewdog-action-setup
37.https://www.bleepingcomputer.com/news/security/github-action-hack-likely-led-to-another-in-cascading-supply-chain-attack/
38.https://www.bankinfosecurity.com/second-github-actions-supply-chain-attack-discovered-a-27751
39.https://www.bitdefender.com/en-us/blog/businessinsights/technical-advisory-update-mass-exploitation-cve-2024-4577
40.https://thehackernews.com/2025/03/hackers-exploit-severe-php-flaw-to.html