CertVu

DCDT

MONTHLY BULLETIN

Cert Vanuatu Security Bulletin

January
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!

"Security is always excessive until it's not enough." — Robbie Sinclair

OVERVIEW

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

CERT VANUATU EFFORTS

CERT Vanuatu (CERT-VU) plays a crucial role in strengthening Vanuatu's cybersecurity efforts. Through close collaboration with diverse stakeholders, CERT-VU addresses cybersecurity challenges at multiple levels, striving to build a well-informed and resilient community against cyber threats.

CERTVU OPERATIONS

INTERNATIONAL COLLABORATION

CERT Vanuatu (CERT-VU) remains dedicated to enhancing its international partnerships, striving to strengthen its presence in the global cybersecurity landscape. By collaborating with cybersecurity organizations across the Pacific and beyond, CERT-VU actively exchanges knowledge and best practices to enhance its capabilities.

Through ongoing participation in joint projects and information-sharing forums, CERT-VU plays a vital role in fostering long-term international cooperation, contributing to a more secure digital environment for Vanuatu and the global community.

INCIDENT RESPONSE

CERTVU maintains a proactive incident response team dedicated to managing daily cyber threats. This team plays a vital role in defending against advanced cyberattacks, including phishing, ransomware, malware, and social engineering tactics.

Phishing remains the most prevalent and effective threat, accounting for nearly 50% of all incidents handled by the team. This underscores both the widespread nature of phishing attacks and the growing emphasis cybercriminals place on exploiting human vulnerabilities to bypass security defenses

MULTI-STAKEHOLDER

Family I ready Program With World Vision

The Family i Ready (FIR) Program by World Vision is designed to support families in Vanuatu who are preparing for seasonal work under the Recognised Seasonal Employer (RSE) scheme in New Zealand and the Pacific Australia Labour Mobility (PALM) scheme in Australia. The program focuses on helping workers and their families back home build financial literacy, strengthen family resilience, and improve communication during their time apart.

Last year, the Department of Cybersecurity and Digital Transformation (DCDT) actively contributed to the program by supporting digital communication initiatives, cybersecurity awareness, and access to secure online platforms. This year, DCDT will continue its involvement, ensuring that families remain digitally connected, informed, and resilient while their loved ones work abroad. This ongoing partnership underscores a commitment to leveraging technology to support the well-being of seasonal workers and their families in Vanuatu.

CYBER SECURITY AWARENESS PROGRAM

CERTVU continues to host its weekly radio program every Friday, focusing on cybersecurity awareness and digital safety.

This initiative aims to keep the public informed about the latest cyber threats and best practices for online security.

For the most current updates and detailed information, I recommend visiting CERTVU's official Facebook page or tuning in to their one hour Friday broadcasts from 8am to 9am.

DCDT DISASTER OPERATIONS

COMMUNITY WIFI DURING THE

During the earthquake recovery in Port Vila, the Department of Cybersecurity and Digital Transformation (DCDT) played a crucial role in restoring connectivity for affected communities. To ensure residents had access to vital online resources, emergency services, and communication channels, DCDT deployed Starlink devices across various locations around Port Vila. This initiative helped bridge the connectivity gap, providing much-needed internet access to support recovery efforts and keep communities informed during the crisis.

VULNERABILITIES AND ACTIVE EXPLOITS

1.MAJOR VULNERABILITIES PATCHED IN SONICWALL, PALO ALTO EXPEDITION, AND AVIATRIX CONTROLLERS

"Palo Alto Networks has released software patches to address several security flaws in its Expedition migration tool, including a high-severity bug that an authenticated attacker could exploit to access sensitive data. "Multiple vulnerabilities in the Palo Alto Networks Expedition migration tool enable an attacker to read Expedition database contents and arbitrary files, as well as create and delete arbitrary files on the Expedition system," the company said in an advisory. "These files include information such as usernames, cleartext passwords, device configurations, and device API keys for firewalls running PAN-OS software."

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

https://the hackernews.com/2025/01/major-vulnerability-patched-in.html
https://security.paloaltonetworks.com/PAN-SA_2025-0001

2.WIZ RESEARCH IDENTIFIES EXPLOITATION IN THE WILD OF AVIATRIX CONTROLLER RCE (CVE-2024-50603)

"CVE-2024-50603 is a critical code execution vulnerability impacting Aviatrix Controller with the maximum CVSS score of 10.0. This command injection flaw allows unauthenticated attackers to execute arbitrary commands on the system remotely. The vulnerability stems from the improper neutralization of user-supplied input, and has been addressed in patched versions 7.1.4191 and 7.2.4996."

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

https://www.wiz.io/blog/wiz-research-identifies-exploitation-in-the-wild-of-aviatrix-cve-2024-50603

3.SAP PATCHES CRITICAL VULNERABILITIES IN NETWEAVER

"Enterprise software maker SAP on Tuesday announced the release of 14 new security notes as part of its January 2025 Patch Day. The most important of the notes are marked ‘hot news’ (the highest SAP severity rating) and address two critical vulnerabilities in NetWeaver AS for ABAP and ABAP Platform, both with a CVSS score of 9.9. Tracked as CVE-2025-0070, the first of the security defects is described as an improper authentication bug. It could allow an attacker to steal credentials from the internal RFC communication between an HTTP client and a server of the same system."

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

https://www.securityweek.com/sap-patches-critical-vulnerabilities-in-netweaver

4.IVANTI RELEASES SECURITY UPDATES FOR MULTIPLE PRODUCTS

"Ivanti released security updates to address vulnerabilities in Ivanti Avalanche, Ivanti Application Control Engine, and Ivanti EPM."

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

https://www.cisa.gov/news-events/alerts/2025/01/14/ivanti-releases-security-updates-multiple-products

5.CISCO FIXES CRITICAL PRIVILEGE ESCALATION FLAW IN MEETING MANAGEMENT (CVSS 9.9)

"Cisco has released software updates to address a critical security flaw impacting Meeting Management that could permit a remote, authenticated attacker to gain administrator privileges on susceptible instances. The vulnerability, tracked as CVE-2025-20156, carries a CVSS score of 9.9 out 10.0. It has been described as a privilege escalation flaw in the REST API of Cisco Meeting Management. "This vulnerability exists because proper authorization is not enforced upon REST API users," the company said in a Wednesday advisory. "An attacker could exploit this vulnerability by sending API requests to a specific endpoint."

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

https://thehackernews.com/2025/01/cisco-fixes-critical-privilege.html>

VULNERABILITIES AND ACTIVE EXPLOITS

6. SONICWALL WARNS OF SMA1000 RCE FLAW EXPLOITED IN ZERO-DAY ATTACKS

"SonicWall is warning about a pre-authentication deserialization vulnerability in SonicWall SMA1000 Appliance Management Console (AMC) and Central Management Console (CMC), with reports that it has been exploited as a zero-day in attacks. The flaw, tracked as CVE-2025-23006 and rated critical (CVSS v3 score: 9.8), could allow remote unauthenticated attackers to execute arbitrary OS commands under specific conditions. The vulnerability affects all firmware versions of the SMA100 appliance up to 12.4.3- 02804 (platform-hotfix)."

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

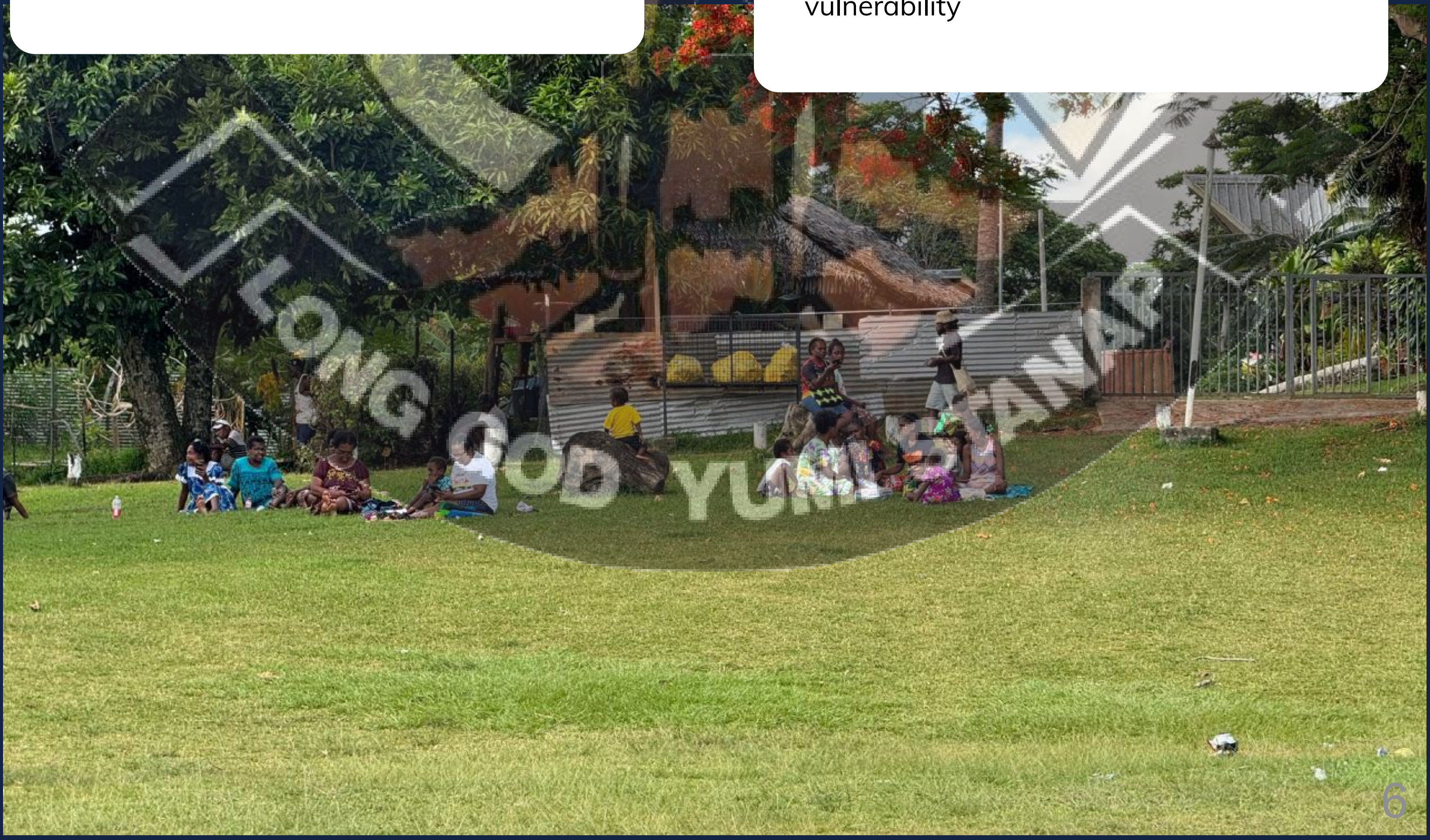
https://www.bleepingcomputer.com/news/security/sonicwall-warns-of-sma1000-rce-flaw-exploited-in-zero-day-attacks/

7.CISCO FIXES CRITICAL VULNERABILITY IN MEETING MANAGEMENT

"Cisco has warned about a new privilege escalation vulnerability in its Meeting Management tool that could allow a remote attacker to gain administrator privileges on exposed instances. The vulnerability, CVE-2025-20156, was disclosed by Cisco on January 22 and is awaiting further analysis by the US National Vulnerability Database (NVD). Cisco also issued a security advisory the same day, allocating the flaw a severity score (CVSS) of 9.9, meaning it is a critical vulnerability."

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

https:www.infosecurity-magazine.com/news/cisco-critical-vulnerability



SECURITY ADVISORIES

ADVISORY 75: MICROSOFT PUBLISHER SECURITY FEATURE BYPASS VULNERABILITY

Microsoft released security updates to address vulnerabilities in multiple Microsoft products. A cyber threat actor could exploit some of these vulnerabilities to take control of an affected system.

https://cert.gov.vu/index.php/services/online-advisories-alerts/243-advisory-75

ADVISORY 76: SONICWALL VULNERABILITY - CVE-2025-23006

Pre-authentication deserialization of untrusted data vulnerability has been identified in the SMA1000 Appliance Management Console (AMC) and Central Management Console (CMC), which in specific conditions could potentially enable a remote unauthenticated attacker to execute arbitrary OS commands.

https://cert.gov.vu/index.php/services/online-advisories-alerts/245-advisory-76

h

MALWARE

1.HACKERS EXPLOIT KERIOCONTROL FIREWALL FLAW TO STEAL ADMIN CSRF TOKENS

"Hackers are trying to exploit CVE-2024-52875, a critical CRLF injection vulnerability that leads to 1- click remote code execution (RCE) attacks in GFI KerioControl firewall product. KerioControl is a network security solution designed for small and medium-sized businesses that combines firewall, VPN, bandwidth management, reporting and monitoring, traffic filtering, AV protection, and intrusion prevention. On December 16, 2024, security researcher Egidio Romano (EgiX) published a detailed writeup on CVE-2024-52875, demonstrating how a seemingly low-severity HTTP response splitting problem could escalate to 1-click RCE."

https://www.bleepingcomputer.com/news/security/hackers-exploit-keriocontrol-firewall-flaw-to-steal-admin-csrf-tokens/>

2. IVANTI CONNECT SECURE VPN TARGETED IN NEW ZERO-DAY EXPLOITATION

"On Wednesday, Jan. 8, 2025, Ivanti disclosed two vulnerabilities, CVE-2025-0282 and CVE-2025-0283, impacting Ivanti Connect Secure ("ICS") VPN appliances. Mandiant has identified zero-day exploitation of CVE-2025-0282 in the wild beginning mid-December 2024. CVE-2025-0282 is an unauthenticated stack-based buffer overflow. Successful exploitation could result in unauthenticated remote code execution, leading to potential downstream compromise of a victim network."

https://cloud.google.com/blog/topics/threat-intelligence/ivanti-connect-secure-vpn-zero-day

3.CONSOLE CHAOS: A CAMPAIGN TARGETING PUBLICLY EXPOSED MANAGEMENT INTERFACES ON FORTINET FORTIGATE FIREWALLS

"In early December, Arctic Wolf Labs began observing a campaign involving suspicious activity on Fortinet FortiGate firewall devices. By gaining access to management interfaces on affected firewalls, threat actors were able to alter firewall configurations. In compromised environments, threat actors were observed extracting credentials using DCSync. While the initial access vector used in this campaign is not yet confirmed, Arctic Wolf Labs assesses with high confidence that mass exploitation of a zero-day vulnerability is likely given the compressed timeline across affected organizations as well as firmware versions affected."

https://arcticwolf.com/resources/blog/console-chaos-targets-fortinet-fortigate-firewalls/>

REFERENCES

1.https://www.bleepingcomputer.com/news/security/hackers-exploit-keriocontrol-firewall-flaw-to-steal-admin-csrf-tokens/
2.https://censys.com/cve-2024-52875/
3.https://viz.greynoise.io/tags/kerio-control-cve-2024-52875-crlf-injection-attempt?days=10
4.https://cloud.google.com/blog/topics/threat-intelligence/ivanti-connect-secure-vpn-zero-day
5.https://www.bleepingcomputer.com/news/security/google-chinese-hackers-likely-behind-ivanti-vpn-zero-day-attacks/
6.https://therecord.media/china-espionage-ivanti-vulnerabilities-mandiant
7.https://cyberscoop.com/ivanti-vpn-vulnerabilities-zero-day-exploit-china-cisa/
8.https://cyberscoop.com/ivanti-vpn-vulnerabilities-zero-day-exploit-china-cisa/
9.https://www.helpnetsecurity.com/2025/01/09/ivanti-cve-2025-0282-zero-day-attacks-indicators-of-compromise/>
10. https://www.wiz.io/blog/wiz-research-identifies-exploitation-in-the-wild-of-aviatrix-cve-2024-50603
11.https://thehackernews.com/2025/01/hackers-exploit-aviatrix-controller.html>
12.https://www.bleepingcomputer.com/news/security/hackers-exploit-critical-aviatrix-controller-rce-flaw-in-attacks/>
13.https://www.darkreading.com/cloud-security/cloud-attackers-exploit-max-critical-aviatrix-rce-flaw>
14.https://www.theregister.com/2025/01/13/severe_aviatrix_controller_vulnerability/
15.https://arcticwolf.com/resources/blog/console-chaos-targets-fortinet-fortigate-firewalls/>
16.https://threats.wiz.io/all-incidents/campaign-targeting-publicly-exposed-management-interfaces-on-fortinet-fortigate-firewalls\
17.https://www.theregister.com/2025/01/14/miscreants_mass_exploited_fortinet_firewalls/
18.https://www.securityweek.com/sap-patches-critical-vulnerabilities-in-netweaver/
19.https://www.cisa.gov/news-events/alerts/2025/01/14/ivanti-releases-security-updates-multiple-products
20.https://forums.ivanti.com/s/article/Security-Advisory-Ivanti-Avalanche-6-4-7-Multiple-CVEs
21.https://forums.ivanti.com/s/article/Security-Advisory-Ivanti-Application-Control-Engine-CVE-2024-10630
22.https://forums.ivanti.com/s/article/Security-Advisory-EPM-January-2025-for-EPM-2024-and-EPM-2022-SU6
23.https://www.securityweek.com/ivanti-patches-critical-vulnerabilities-in-endpoint-manager-2/
24.https://www.bleepingcomputer.com/news/security/sonicwall-warns-of-sma1000-rce-flaw-exploited-in-zero-day-attacks/
25.https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2025-0002
26.https://thehackernews.com/2025/01/sonicwall-urges-immediate-patch-for.html
27.https://cyberscoop.com/sonicwall-sma-zero-day-patch/
28.https://www.securityweek.com/sonicwall-learns-from-microsoft-about-potentially-exploited-zero-day/
29.https://www.helpnetsecurity.com/2025/01/23/sonicwall-sma-1000-exploited-zero-day-cve-2025-23006/
30.https://www.theregister.com/2025/01/23/sonicwall_critical_bug/
31.https://www.infosecurity-magazine.com/news/cisco-critical-vulnerability/
32.https://thehackernews.com/2025/01/cisco-fixes-critical-privilege.html
33.https://www.securityweek.com/cisco-patches-critical-vulnerability-in-meeting-management/
34.https://cert.gov.vu/index.php/services/online-advisories-alerts
35.https://www.facebook.com/CERTVU