MONTHLY BULLETIN

Cert Vanuatu Security Bulletin

February
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 isn't a finish line; it's a constant chase against the unseen."
CERTVU

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 February 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

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.

Muti – Stakeholder Meeting- Between Department of Communications and Digital Transformation and Vanuatu Bureau of Standards

On 24 February 2025, the Department of Communication and Digital Transformation (DCDT) held an initial discussion with the Vanuatu Bureau of Standards (VBS) regarding the adoption and implementation of the SMB1001 standard. This standard is closely linked to ISO 27001, an internationally recognized framework for information security management systems (ISMS), to which VBS has subscribed.

The discussion focused on ensuring that SMB1001 and ISO 27001 align with the Vanuatu Government Digital Master Plan, which serves as a strategic framework for the country's digital transformation initiatives. By integrating these standards, the government aims to enhance cybersecurity measures, improve data protection, and establish robust governance structures for digital services.

The meeting also explored the potential benefits of adopting both standards, including strengthening national cybersecurity resilience, fostering trust in digital services, and ensuring compliance with international best practices. Moving forward, DCDT and VBS will continue collaborating to implement these standards effectively, providing a secure and efficient foundation for Vanuatu's digital future.

CERTVU OPERATIONS

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

CYBERSECURITY CAPACITY BUILDING

Two staff members from the Department of Cybersecurity, Digital Transformation & Telecommunications (DCDT) attended a cybersecurity training program in Guam from February 6 to 14, 2025. This training was an initiative under the CERTVU operation, focused on building the capacity of DCDT staff in cybersecurity incident detection and response. The program was sponsored by the Ministry of Internal Affairs and Communications (MIC) of Japan, reinforcing international collaboration in cybersecurity.

The training primarily covered:

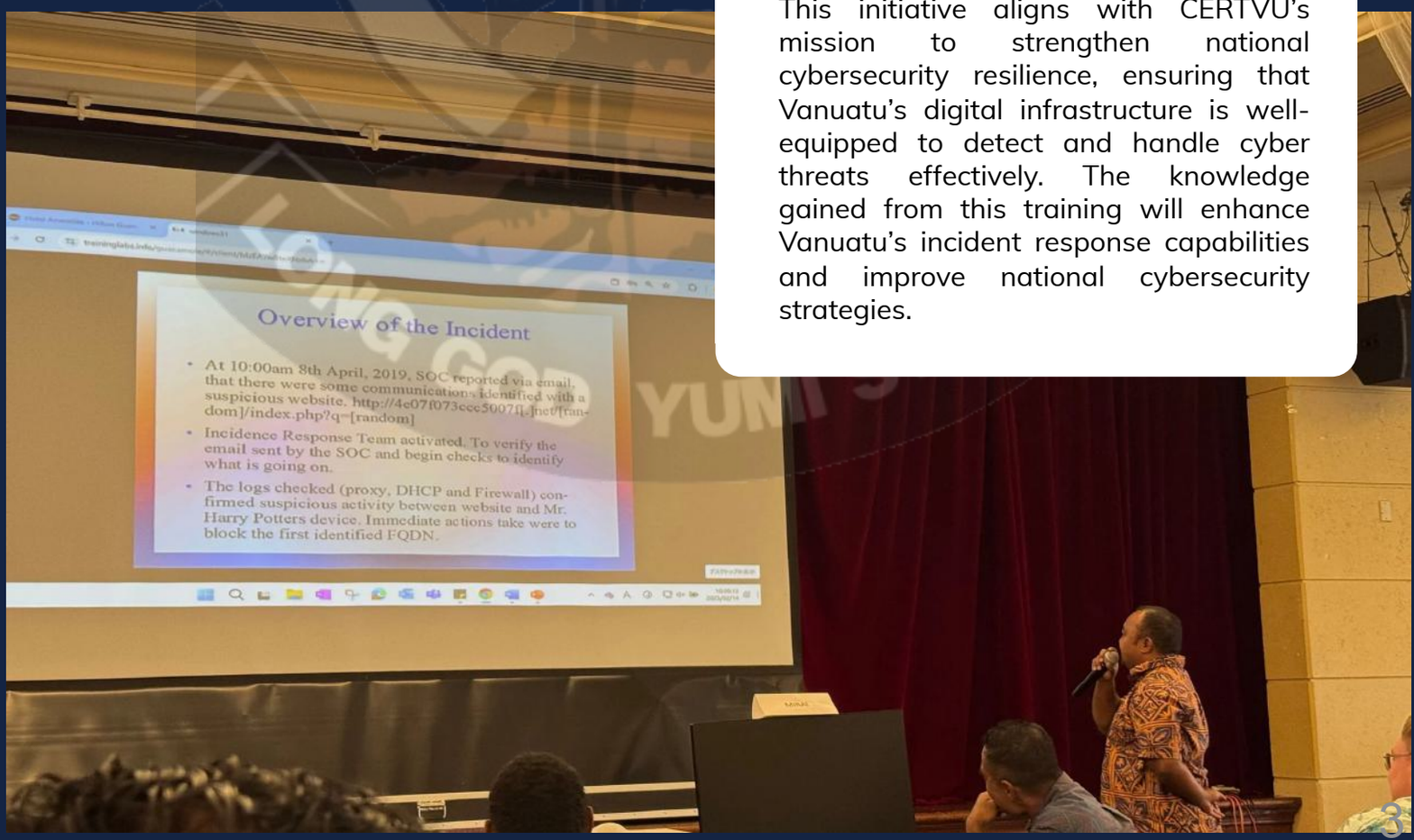
Incident Detection – Identifying cyber threats, analyzing attack patterns, and monitoring network activity.

Incident Response – Implementing effective response strategies to contain and mitigate cyber incidents.

Digital Forensics – Investigating security breaches and gathering forensic evidence.

Threat Intelligence – Understanding emerging cyber risks and proactive defense mechanisms.

This initiative aligns with CERTVU's mission to strengthen national cybersecurity resilience, ensuring that Vanuatu's digital infrastructure is well-equipped to detect and handle cyber threats effectively. The knowledge gained from this training will enhance Vanuatu's incident response capabilities and improve national cybersecurity strategies.



CERTVU OPERATIONS

INTERNATIONAL COLLABORATION

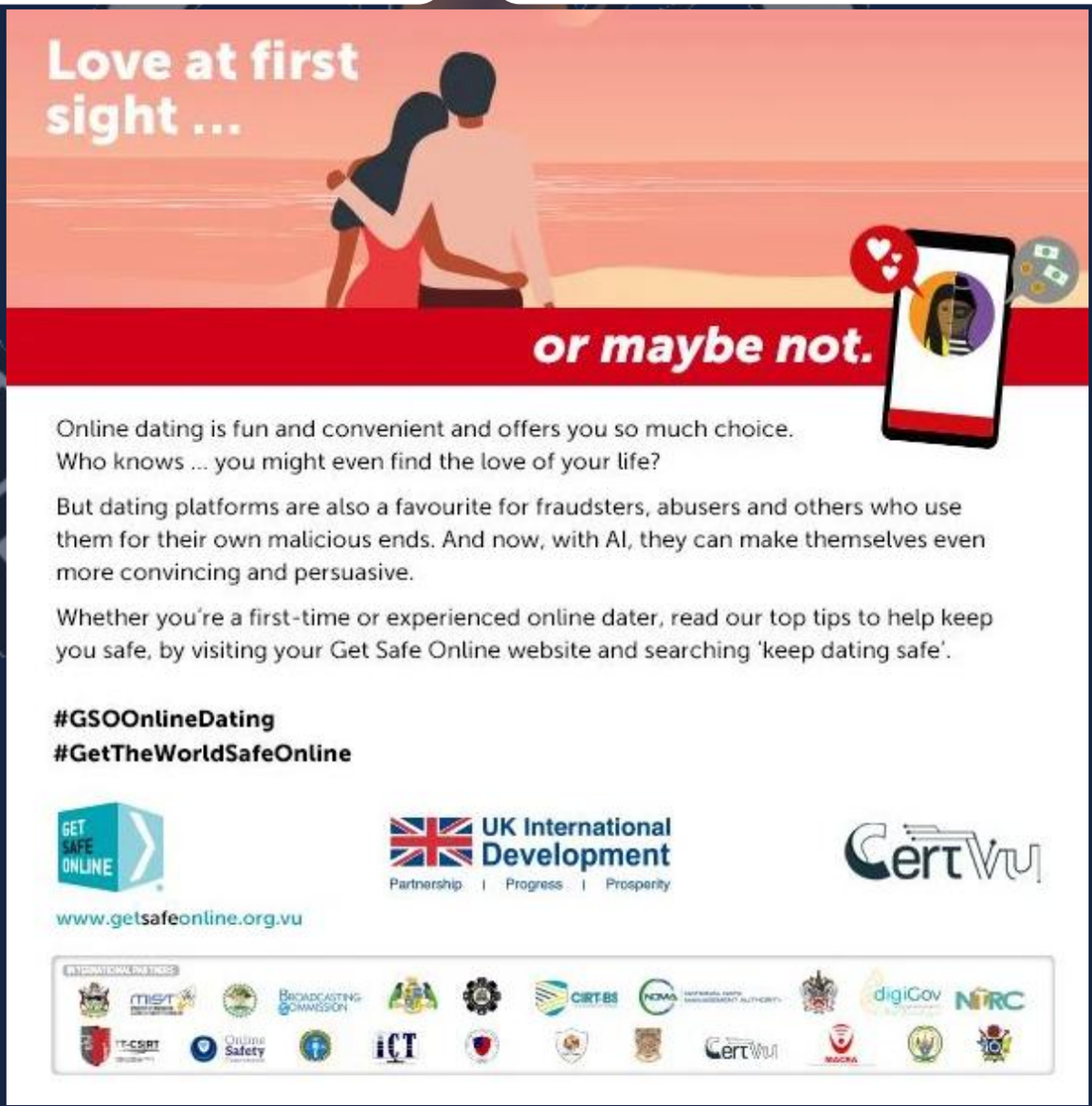
CERT Vanuatu (CERT-VU) remains dedicated to enhancing its international partnerships, striving to strengthen its presence in the global cybersecurity landscape. By collaborating with cybersecurity organizations across the Pacific and beyond, CERT-VU actively exchanges knowledge and best practices to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

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.



VULNERABILITIES AND ACTIVE EXPLOITS

1.MITRE CALDERA SECURITY ADVISORY — REMOTE CODE EXECUTION (CVE-2025–27364)

"All versions of MITRE Caldera (before commit 35bc06e and going back as far as the very first versions of Caldera) are vulnerable to a remote code execution (RCE) vulnerability that can be triggered in most default configurations. The only preconditions for this vulnerability to be exploitable are the presence of Go, python and gcc on the system that the Caldera server is running on. Notably, all of these dependencies are required for Caldera to be fully-functional in the first place and on many distributions, gcc is a dependency of Go, meaning this vulnerability is extremely likely to be available to an attacker."

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

https://medium.com/@mitrecaldera/mitre-caldera-security-advisory-remote-code-execution-cve-2025-27364-5f679e2e2a0e

2.100,000 WORDPRESS SITES AFFECTED BY ARBITRARY FILE UPLOAD, READ AND DELETION VULNERABILITY IN EVEREST FORMS WORDPRESS PLUGIN

"On January 16th, 2025, we received a submission for an Arbitrary File Upload vulnerability in Everest Forms, a WordPress plugin with more than 100,000 active installations. This vulnerability makes it possible for an unauthenticated attacker to upload arbitrary files to a vulnerable site and achieve remote code execution, and also makes it possible for unauthenticated threat actors to read and delete arbitrary files, including the wp-config.php file, which can make site takeover possible."

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

https://www.wordfence.com/blog/2025/02/100000-wordpress-sites-affected-by-arbitrary-file-upload-read-and-deletion-vulnerability-in-everest-forms-wordpress-plugin/

VULNERABILITIES AND ACTIVE EXPLOITS

3.ATLASSIAN PATCHES CRITICAL VULNERABILITIES IN CONFLUENCE, CROWD

"Atlassian this week announced the rollout of patches for 12 critical- and high-severity vulnerabilities in its Bamboo, Bitbucket, Confluence, Crowd, and Jira products. The company released fixes for five critical-severity issues in Confluence Data Center and Server and Crowd Data Center and Server that were discovered in third-party dependencies used within the two products. Updates released for 2/8 Confluence Data Center and Server address two critical flaws in Apache Tomcat. Tracked as CVE-2024- 50379 and CVE-2024-56337 (CVSS score of 9.8), the two issues could be exploited by unauthenticated attackers to achieve remote code execution (RCE), the company warns."

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

https://www.securityweek.com/atlassian-patches-critical-vulnerabilities-in-confluence-crowd/

4.JUNIPER PATCHES CRITICAL AUTH BYPASS IN SESSION SMART ROUTERS

"Juniper Networks has patched a critical vulnerability that allows attackers to bypass authentication and take over Session Smart Router (SSR) devices. The security flaw (tracked as CVE-2025-21589) was found during internal product security testing, and it also affects Session Smart Conductor and WAN Assurance Managed Routers. "An Authentication Bypass Using an Alternate Path or Channel vulnerability in Juniper Networks Session Smart Router may allow a network-based attacker to bypass authentication and take administrative control of the device," the American networking infrastructure company said in an out-of-cycle security advisory released last week."

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/juniper-patches-critical-auth-bypass-in-session-smart-routers/>

VULNERABILITIES AND ACTIVE EXPLOITS

5.IVANTI PATCHES CRITICAL FLAWS IN CONNECT SECURE AND POLICY SECURE – UPDATE NOW

"Ivanti has released security updates to address multiple security flaws impacting Connect Secure (ICS), Policy Secure (IPS), and Cloud Services Application (CSA) that could be exploited to achieve arbitrary code execution."

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

https://thehackernews.com/2025/02/ivanti-patches-critical-flaws-in.html

6.ZIMBRA RELEASES SECURITY UPDATES FOR SQL INJECTION, STORED XSS, AND SSRF VULNERABILITIES

"Zimbra has released software updates to address critical security flaws in its Collaboration software that, if successfully exploited, could result in information disclosure under certain conditions. The vulnerability, tracked as CVE-2025-25064, carries a CVSS score of 9.8 out of a maximum of 10.0. It has been described as an SQL injection bug in the ZimbraSync Service SOAP endpoint affecting versions prior to 10.0.12 and 10.1.4. Stemming from a lack of adequate sanitization of a user-supplied parameter, the shortcoming could be weaponized by authenticated attackers to inject arbitrary SQL queries that could retrieve email metadata by "manipulating a specific parameter in the request."

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

https://thehackernews.com/2025/02/zimbra-releases-security-updates-for.html

VULNERABILITIES AND ACTIVE EXPLOITS

7.CRITICAL CISCO ISE BUG CAN LET ATTACKERS RUN COMMANDS AS ROOT

"Cisco has released patches to fix two critical vulnerabilities in its Identity Services Engine (ISE) security policy management platform. Enterprise administrators use Cisco ISE as an identity and access management (IAM) solution that combines authentication, authorization, and accounting into a single appliance. The two security flaws (CVE-2025-20124 and CVE-2025-20125) can be exploited by authenticated remote attackers with read-only admin privileges to execute arbitrary commands as root and bypass authorization on unpatched devices."

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-cisco-ise-bug-can-let-attackers-run-commands-as-root/

8.MICROSOFT PATCHES CRITICAL AZURE AI FACE SERVICE VULNERABILITY WITH CVSS 9.9 SCORE

"Microsoft has released patches to address two Critical-rated security flaws impacting Azure AI Face Service and Microsoft Account that could allow a malicious actor to escalate their privileges under certain conditions."

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

https://thehackernews.com/2025/02/microsoft-patches-critical-azure-ai.html

9.NETGEAR WARNS USERS TO PATCH CRITICAL WIFI ROUTER VULNERABILITIES

"Netgear has fixed two critical vulnerabilities affecting multiple WiFi router models and urged customers to update their devices to the latest firmware as soon as possible. The security flaws impact multiple WiFi 6 access points (WAX206, WAX214v2, and WAX220) and Nighthawk Pro Gaming router models (XR1000, XR1000v2, XR500). Although the American computer networking company did not disclose more details about the two bugs, it did reveal that unauthenticated threat actors can exploit them for remote code execution (tracked internally as PSV-2023-0039) and authentication bypass (PSV-2021- 0117) in low-complexity attacks that don't require user interaction."

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/netgear-warns-users-to-patch-critical-wifi-router-vulnerabilities/

SECURITY ADVISORIES

ADVISORY 77: FORTIOS & FORTIPROXY - AUTHENTICATION BYPASS IN NODE.JS WEB SOCKET MODULE VULNERABILITY

Fortinet has identified a critical vulnerability in FortiOS and FortiProxy. The vulnerability may allow an unauthenticated remote attacker to gain “super-admin” privileges.

- The Fortinet vulnerability notification describes possible Indicators of Compromise (IOCs) and IPs associated with the threat actor, which may assist in identifying suspicious activity.
- Fortinet has observed active exploitation of this vulnerability.
- Fortinet advises that threat actors have been observed performing the following post-exploitation activities:
- Creating an admin account on the device with a random username.
- Creating a Local User account on the device using a random name.
- Creating a user group or adding the above local user to an existing SSL VPN user group.
- Adding/changing other settings (firewall policy etc.)
- Logging in the SSL-VPN with the above-added local users to get a tunnel to the internal network.

https://cert.gov.vu/index.php/services/online-advisories-alerts/246-advisory-77

ADVISORY 78: VEEAM RELEASES SECURITY UPDATES FOR MULTIPLE PRODUCTS

eeam released security updates to address vulnerabilities in multiple products. A vulnerability in the Veeam Updater component allows an attacker to use a Man-in-the-Middle attack to execute arbitrary code on the affected appliance server with root-level permissions. CERTVU encourages all System administrators to review the following advisory and apply necessary updates.

https://cert.gov.vu/index.php/services/online-advisories-alerts/248-advisory-78

ADVISORY 79: TRIMBLE RELEASES SECURITY UPDATES TO ADDRESS A VULNERABILITY IMPACTING ITS CITYWORKS SERVER AMS

Trimble has released security updates for vulnerability (CVE-2025-0994) impacting its Cityworks Server AMS (Asset Management System).

https://cert.gov.vu/index.php/services/online-advisories-alerts/249-advisory-79

ADVISORY 80: SONICWALL VULNERABILITY – CVE-2024-53704

SonicWALL SonicOS contains an improper authentication vulnerability in the SSLVPN authentication mechanism that allows a remote attacker to bypass authentication.

https://cert.gov.vu/index.php/services/online-advisories-alerts/250-advisory-80

MALWARE

1.PALO ALTO NETWORKS TAGS NEW FIREWALL BUG AS EXPLOITED IN ATTACKS

"Palo Alto Networks warns that a file read vulnerability (CVE-2025-0111) is now being chained in attacks with two other flaws (CVE-2025-0108 with CVE-2024-9474) to breach PAN-OS firewalls in active attacks. The vendor first disclosed the authentication bypass vulnerability tracked as CVE-2025-0108 on February 12, 2025, releasing patches to fix the vulnerability. That same day, Assetnote researchers published a proof-of-concept exploit demonstrating how CVE-2025-0108 and CVE-2024-9474 could be chained together to gain root privileges on unpatched PAN-OS firewalls. A day later, network threat intel firm GreyNoise reported that threat actors had begun actively exploiting the flaws, with attempts coming from two IP addresses."

https://www.bleepingcomputer.com/news/security/palo-alto-networks-tags-new-firewall-bug-as-exploited-in-attacks/>

2.ARCTIC WOLF OBSERVES AUTHENTICATION BYPASS EXPLOITATION ATTEMPTS TARGETING SONICWALL FIREWALLS (CVE-2024-53704)

"On February 10, 2025, Bishop Fox published technical details and proof-of-concept (PoC) exploit code for CVE-2024-53704, a high-severity authentication bypass vulnerability caused by a flaw in the SSLVPN authentication mechanism in SonicOS, the operating system used by SonicWall firewalls. Shortly after the PoC was made public, Arctic Wolf began observing exploitation attempts of this vulnerability in the threat landscape."

https://arcticwolf.com/resources/blog/cve-2024-53704/

3.REDMIKE (SALT TYPHOON) EXPLOITS VULNERABLE CISCO DEVICES OF GLOBAL TELECOMMUNICATIONS PROVIDERS

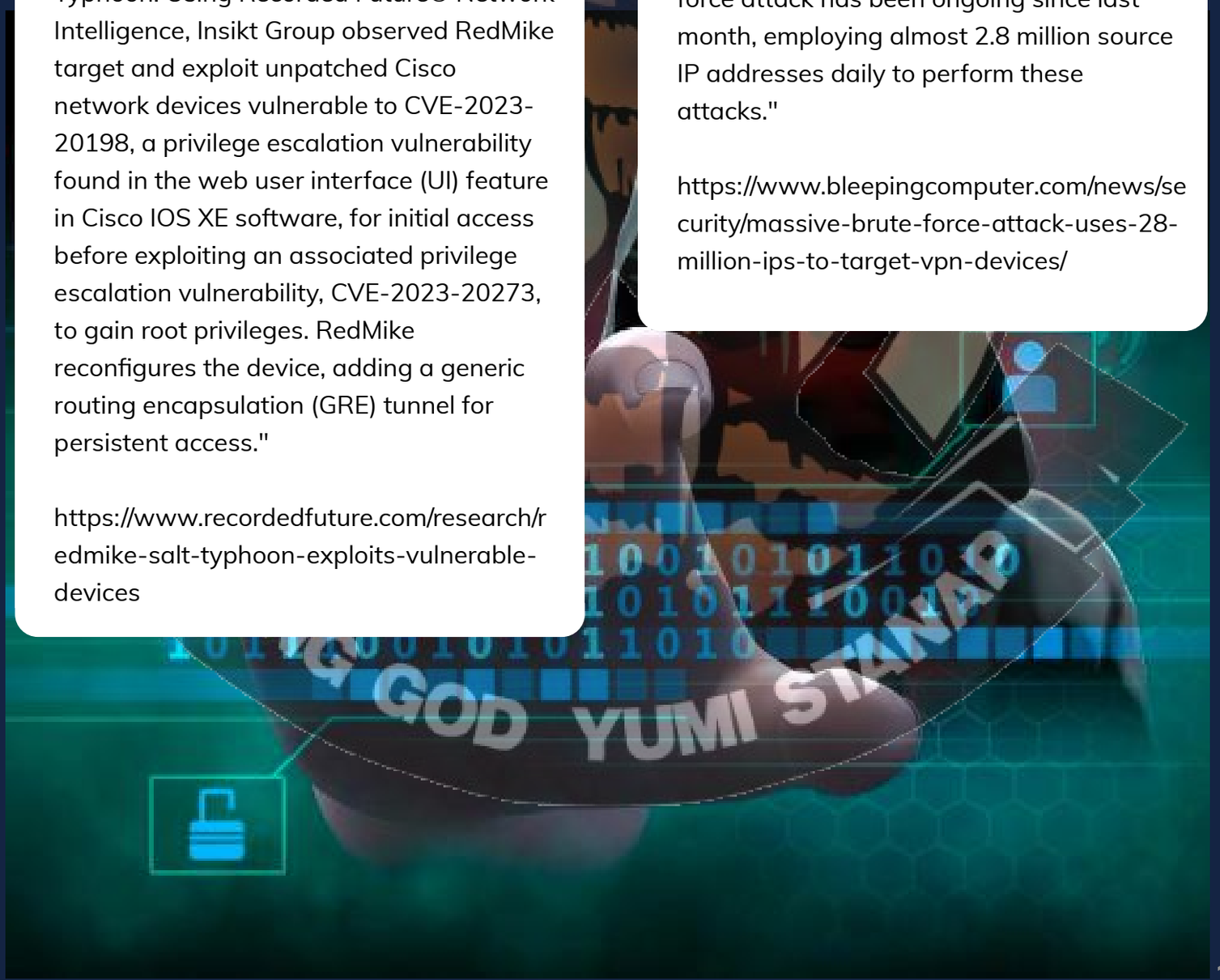
"Between December 2024 and January 2025, Recorded Future's Insikt Group identified a campaign exploiting unpatched internet-facing Cisco network devices primarily associated with global telecommunications providers. Victim organizations included a United States-based affiliate of a United Kingdom-based telecommunications provider and a South African telecommunications provider. Insikt Group attributes this activity to the Chinese state-sponsored threat activity group tracked by Insikt Group as RedMike, which aligns with the Microsoft-named group Salt Typhoon. Using Recorded Future® Network Intelligence, Insikt Group observed RedMike target and exploit unpatched Cisco network devices vulnerable to CVE-2023-20198, a privilege escalation vulnerability found in the web user interface (UI) feature in Cisco IOS XE software, for initial access before exploiting an associated privilege escalation vulnerability, CVE-2023-20273, to gain root privileges. RedMike reconfigures the device, adding a generic routing encapsulation (GRE) tunnel for persistent access."

https://www.recordedfuture.com/research/redmike-salt-typhoon-exploits-vulnerable-devices

4.MASSIVE BRUTE FORCE ATTACK USES 2.8 MILLION IPS TO TARGET VPN DEVICES

"A large-scale brute force password attack using almost 2.8 million IP addresses is underway, attempting to guess the credentials for a wide range of networking devices, including those from Palo Alto Networks, Ivanti, and SonicWall. A brute force attack is when threat actors attempt to repeatedly log into an account or device using many usernames and passwords until the correct combination is found. Once they have access to the correct credentials, the threat actors can then use them to hijack a device or gain access to a network. According to the threat monitoring platform The Shadowserver Foundation, a brute force attack has been ongoing since last month, employing almost 2.8 million source IP addresses daily to perform these attacks."

https://www.bleepingcomputer.com/news/security/massive-brute-force-attack-uses-28-million-ips-to-target-vpn-devices/



REFERENCES

1.https://medium.com/@mitrecaldera/mitre-caldera-security-advisory-remote-code-execution-cve-2025-27364-5f679e2e2a0e
2.https://www.darkreading.com/application-security/max-severity-rce-vuln-all-versions-mitre-caldera
3.https://www.theregister.com/2025/02/25/10_bug_mitre_caldera/
4.https://www.wordfence.com/blog/2025/02/100000-wordpress-sites-affected-by-arbitrary-file-upload-read-and-deletion-vulnerability-in-everest-forms-wordpress-plugin/
5.https://www.securityweek.com/atlassian-patches-critical-vulnerabilities-in-confluence-crowd/
6.https://confluence.atlassian.com/security/security-bulletin-february-18-2025-1510670627.html
7.https://www.bleepingcomputer.com/news/security/juniper-patches-critical-auth-bypass-in-session-smart-routers/>
8.https://supportportal.juniper.net/s/article/2025-02-Out-of-Cycle-Security-Bulletin-Session-Smart-Router-Session-Smart-Conductor-WAN-Assurance-Router-API-Authentication-Bypass-Vulnerability-CVE-2025-21589?language=en_US
9.https://thehackernews.com/2025/02/juniper-session-smart-routers.html
10. https://securityaffairs.com/174365/security/juniper-networks-fixed-a-critical-flaw-in-session-smart-routers.html>
11.https://www.securityweek.com/critical-vulnerability-patched-in-juniper-session-smart-router/>
12.https://thehackernews.com/2025/02/ivanti-patches-critical-flaws-in.html
13.https://thehackernews.com/2025/02/ivanti-patches-critical-flaws-in.html
14.https://www.bleepingcomputer.com/news/security/ivanti-fixes-three-critical-flaws-in-connect-secure-and-policy-secure/>
15.https://thehackernews.com/2025/02/zimbra-releases-security-updates-for.html
16.https://www.bleepingcomputer.com/news/security/critical-cisco-ise-bug-can-let-attackers-run-commands-as-root/
17.https://thehackernews.com/2025/02/cisco-patches-critical-ise.html
18.https://thehackernews.com/2025/02/cisco-patches-critical-ise.html
19.https://securityaffairs.com/173946/security/cisco-addressed-critical-flaws-in-identity-services-engine.html
20.https://thehackernews.com/2025/02/microsoft-patches-critical-azure-ai.html
21.https://www.bleepingcomputer.com/news/security/netgear-warns-users-to-patch-critical-wifi-router-vulnerabilities/
22.https://kb.netgear.com/000066557/Security-Advisory-for-Authentication-Bypass-on-Some-Wireless-Access-Points-PSV-2021-0117
23.https://securityaffairs.com/173839/security/netgear-wifi-routers-flaws.html
24.https://www.bleepingcomputer.com/news/security/palo-alto-networks-tags-new-firewall-bug-as-exploited-in-attacks/>
25.https://www.darkreading.com/remote-workforce/patch-now-cisa-researchers-warn-palo-alto-flaw-exploited-wild
26.https://www.greynoise.io/blog/greynoise-observes-active-exploitation-of-pan-os-authentication-bypass-vulnerability-cve-2025-0108
27.https://www.securityweek.com/palo-alto-networks-confirms-exploitation-of-firewall-vulnerability/
28.https://www.securityweek.com/palo-alto-networks-confirms-exploitation-of-firewall-vulnerability/
29.https://www.helpnetsecurity.com/2025/02/19/palo-alto-networks-firewalls-cve-2025-0108-cve-2024-9474-cve-2025-0111/
30.https://arcticwolf.com/resources/blog/cve-2024-53704/
31.https://www.bleepingcomputer.com/news/security/sonicwall-firewall-bug-leveraged-in-attacks-after-poc-exploit-release/
32.https://www.securityweek.com/sonicwall-firewall-vulnerability-exploited-after-poc-publication/
33.https://www.theregister.com/2025/02/14/sonicwall_firewalls_under_attack_patch/
34.https://www.recordedfuture.com/research/redmike-salt-typhoon-exploits-vulnerable-devices
35.https://go.recordedfuture.com/hubfs/reports/cta-cn-2025-0213.pdf
36.https://therecord.media/china-salt-typhoon-cisco-devices
37.https://cyberscoop.com/salt-typhoon-china-ongoing-telecom-attack-spree/
38.https://www.bleepingcomputer.com/news/security/massive-brute-force-attack-uses-28-million-ips-to-target-vpn-devices/
39.https://cert.gov.vu/index.php/services/online-advisories-alerts
40.https://www.facebook.com/CERTVU