MONTHLY BULLETIN

CertVu

DCDT

Cert Vanuatu Security Bulletin

June
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

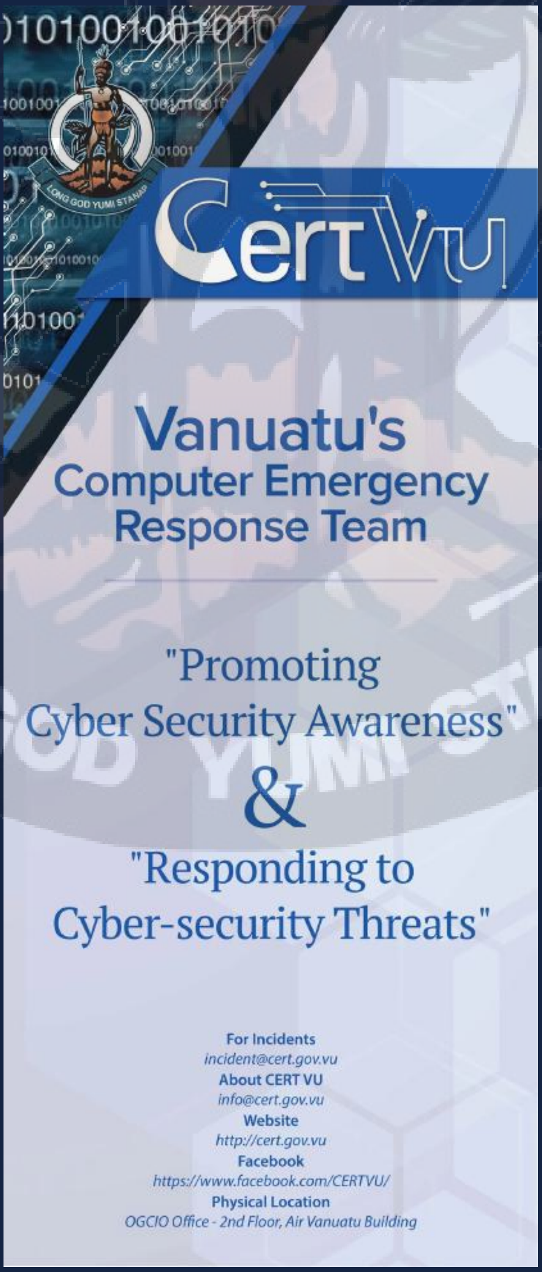
CERT Vanuatu (CERT-VU) continues to strengthen its international partnerships, with a clear focus on enhancing its role in the global cybersecurity landscape. By actively engaging with cybersecurity organizations across the Pacific and beyond, CERT-VU regularly shares knowledge and best practices to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



CertVu
LONG GOD YUMI STANAP

Vanuatu's
Computer Emergency
Response Team

"Promoting
Cyber Security Awareness"
&
"Responding to
Cyber-security Threats"

For Incidents
incident@cert.gov.vu
About CERT VU
info@cert.gov.vu
Website
http://cert.gov.vu
Facebook
https://www.facebook.com/CERTVU/
Physical Location
OGCIO Office - 2nd Floor, Air Vanuatu Building

VULNERABILITIES AND ACTIVE EXPLOITS

1.CISCO WARNS OF ISE AND CCP FLAWS WITH PUBLIC EXPLOIT CODE

"Cisco has released patches to address three vulnerabilities with public exploit code in its Identity Services Engine (ISE) and Customer Collaboration Platform (CCP) solutions. The most severe of the three is a critical static credential vulnerability tracked as CVE-2025-20286, found by GMO Cybersecurity's Kentaro Kawane in Cisco ISE. This identity-based policy enforcement software provides endpoint access control and network device administration in enterprise environments. The vulnerability is due to improperly generated credentials when deploying Cisco ISE on cloud platforms, resulting in shared credentials across different deployments."
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/cisco-warns-of-ise-and-ccp-flaws-with-public-exploit-code/

2.NEW VEEAM RCE FLAW LETS DOMAIN USERS HACK BACKUP SERVERS

"Veeam has released security updates today to fix several Veeam Backup & Replication (VBR) flaws, including a critical remote code execution (RCE) vulnerability. Tracked as CVE-2025-23121, this security flaw was reported by security researchers at watchTowr and CodeWhite, and it only impacts domain‐joined installations. As Veeam explained in a Tuesday security advisory, the vulnerability can be exploited by authenticated domain users in low-complexity attacks to gain code execution remotely on the Backup Server. This flaw affects Veeam Backup & Replication 12 or later, and it was fixed in version 12.3.2.3617, which was released earlier today."
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/new-veeam-rce-flaw-lets-domain-users-hack-backup-servers/

VULNERABILITIES AND ACTIVE EXPLOITS

3.ATTACKERS ACTIVELY EXPLOITING CRITICAL VULNERABILITY IN MOTORS THEME

"On May 2nd, 2025, we received a submission for a Privilege Escalation vulnerability in Motors, a WordPress theme with more than 22,000 sales. This vulnerability makes it possible for an unauthenticated attacker to change the password of any user, including an administrator, which allows them to take over the account and the website. We originally disclosed this vulnerability on May 19th, 2025 and our records indicate that attackers started exploiting the issue the next day on May 20th, 2025. It appears mass exploitation started on June 7th, 2025. The Wordfence Firewall has already blocked over 23,100 exploit attempts targeting this vulnerability."

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

https://www.wordfence.com/blog/2025/06/attackers-actively-exploiting-critical-vulnerability-in-motors-theme/

4.CRITICAL AUTHENTICATION BYPASS FLAW PATCHED IN TELEPORT

"Teleport on Friday warned of a critical-severity vulnerability in the open source platform that can be exploited remotely to bypass standard authentication controls. Teleport provides connectivity, authentication, and access control for servers and cloud applications. It supports protocols such as SSH, RDP, and HTTPS, and can be used with Kubernetes and various databases. Tracked as CVE-2025-49825 (CVSS score of 9.8), the critical flaw can be exploited to circumvent SSH authentication, allowing attackers to access Teleport-managed systems."

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

https://www.securityweek.com/critical-authentication-bypass-flaw-patched-in-teleport/

5.CRITICAL VULNERABILITY EXPOSES MANY MITEL MICOLLAB INSTANCES TO REMOTE HACKING

"Mitel this week informed customers about the availability of patches for a critical MiCollab vulnerability that can be exploited remotely and without authentication. The flaw, which currently does not appear to have a CVE identifier, has been described as a path traversal issue affecting MiCollab's NuPoint Unified Messaging (NPM) component. MiCollab 9.8 SP2 (9.8.2.12) and earlier are impacted, and a patch is included in versions 9.8 SP3 (9.8.3.1) and later. MiCollab 10.0.0.26 and later versions are not affected."
CERTVU recommends all users and organizations to read this advisory and follow the mitigation steps to mitigate these vulnerabilities.

https://www.securityweek.com/critical-vulnerability-exposes-many-mitel-micollab-instances-to-remote-hacking/

6.DON'T CALL THAT "PROTECTED" METHOD: DISSECTING AN N-DAY VBULLETIN RCE

"vBulletin is one of the most widely used commercial forum solutions over the Internet, powering thousands of online communities ranging from niche hobbyist sites to large-scale tech forums. Developed primarily in PHP, it features a custom MVC-like framework and a proprietary API system designed to handle AJAX and mobile app interactions. Over the years, vBulletin has gained a reputation for both its ubiquity and its vulnerability surface — often becoming a prime target for web application exploits."
CERTVU recommends all users and organizations to read this advisory and follow the mitigation steps to mitigate these vulnerabilities.

https://karmainsecurity.com/dont-call-that-protected-method-vbulletin-rce

VULNERABILITIES AND ACTIVE EXPLOITS

7.CISCO IOS XE WLC ARBITRARY FILE UPLOAD VULNERABILITY (CVE-2025-20188) ANALYSIS

"A recent Cisco disclosure detailed a vulnerability affecting Cisco IOS XE Wireless Controller Software version 17.12.03 and earlier. The issue was described as an unauthenticated arbitrary file upload, caused by the presence of a hard-coded JSON Web Token (JWT). Cisco IOS XE Wireless LAN Controller (WLC) is a widely deployed enterprise-grade solution used to manage and control large-scale wireless networks. Integrated into Cisco's IOS XE operating system, it provides centralized management, policy enforcement, and seamless mobility for wireless access points across campus and branch environments."

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

https://horizon3.ai/attack-research/attack-blogs/cisco-ios-xe-wlc-arbitrary-file-upload-vulnerability-cve-2025-20188-analysis/

8.HEWLETT PACKARD ENTERPRISE WARNS OF CRITICAL STOREONCE AUTH BYPASS

"Hewlett Packard Enterprise (HPE) has issued a security bulletin to warn about eight vulnerabilities impacting StoreOnce, its disk-based backup and deduplication solution. Among the flaws fixed this time is a critical severity (CVSS v3.1 score: 9.8) authentication bypass vulnerability tracked under CVE-2025- 37093, three remote code execution bugs, two directory traversal problems, and a server-side request forgery issue. The flaws impact all versions of the HPE StoreOnce Software before v4.3.11, which is now the recommended upgrade version."

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/hewlett-packard-enterprise-warns-of-critical-storeonce-auth-bypass/

MALWARE

1.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/

2.CRITICAL FORTINET FLAWS NOW EXPLOITED IN QILIN RANSOMWARE ATTACKS

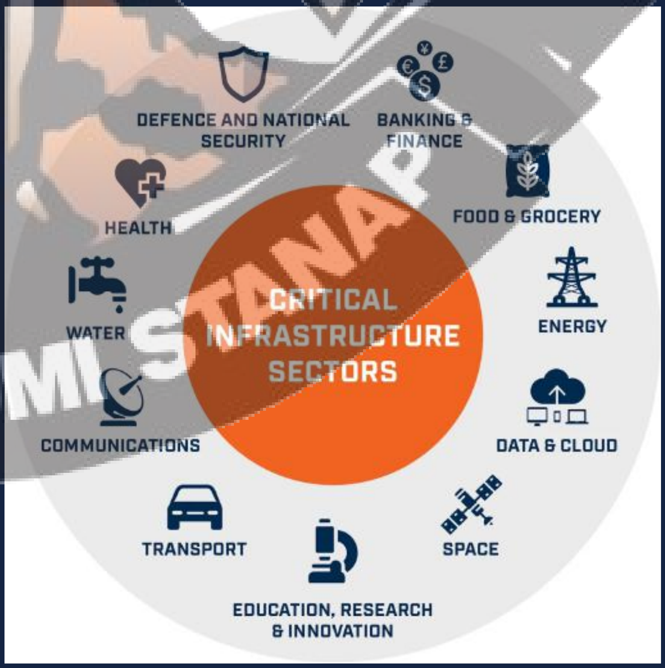
"The Qilin ransomware operation has recently joined attacks exploiting two Fortinet vulnerabilities that allow bypassing authentication on vulnerable devices and executing malicious code remotely. Qilin (also tracked as Phantom Mantis) surfaced in August 2022 as a Ransomware-as-a-Service (RaaS) operation under the "Agenda" name and has since claimed responsibility for over 310 victims on its dark web leak site. Its victim list also includes high-profile organizations, such as automotive giant Yangfeng, publishing giant Lee Enterprises, Australia's Court Services Victoria, and pathology services provider Synnovis. The Synnovis incident impacted several major NHS hospitals in London, which forced them to cancel hundreds of appointments and operations."

https://www.bleepingcomputer.com/news/security/critical-fortinet-flaws-now-exploited-in-qilin-ransomware-attacks/

3.FOLLOW THE SMOKE | CHINA-NEXUS THREAT ACTORS HAMMER AT THE DOORS OF TOP TIER TARGETS

"This research outlines threats that SentinelLABS observed and defended against in late 2024 and the first quarter of 2025. This post expands upon previous SentinelLABS research, which provides an overview of threats against cybersecurity vendors, including SentinelOne, ranging from financially motivated crimeware to targeted attacks by nation-state actors. This research focuses specifically on the subset of threats targeting SentinelOne and others that we attribute to China-nexus threat actors."

https://hackread.com/chinese-linked-hackers-targeted-global-organizations/

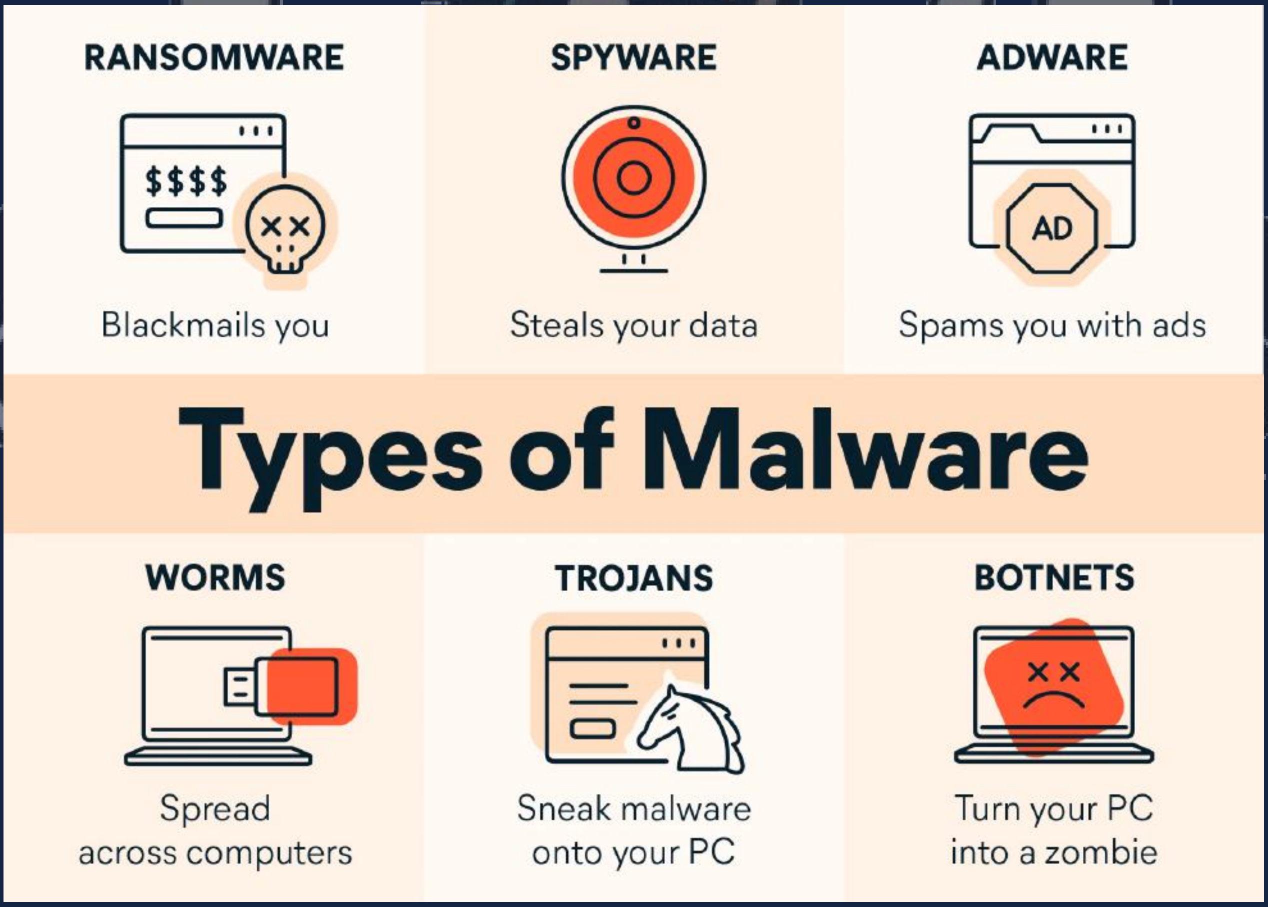


MALWARE

4.THREAT SPOTLIGHT: CVE-2025-5777: CITRIX BLEED 2 OPENS OLD WOUNDS

"Citrix released an advisory for CVE-2025-5777 affecting NetScaler ADC and Gateway devices, allowing attackers to hijack user sessions and bypass authentication. While no public reporting of exploitation for this vulnerability has emerged, ReliaQuest has observed indications of exploitation to gain initial access. Citrix recommends patching affected systems to the latest versions and terminating active sessions to mitigate session hijacking and further risks of exploitation."

https://reliaquest.com/blog/threat-spotlight-citrix-bleed-2-vulnerability-in-netscaler-adc-gateway-devices/



RANSOMWARE

Blackmails you

SPYWARE

Steals your data

ADWARE

Spams you with ads

Types of Malware

WORMS

Spread across computers

TROJANS

Sneak malware onto your PC

BOTNETS

Turn your PC into a zombie

REFERENCES

1.https://www.bleepingcomputer.com/news/security/cisco-warns-of-ise-and-ccp-flaws-with-public-exploit-code/
2.https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ise-aws-static-cred-FPMjUcm7
3.https://www.bleepingcomputer.com/news/security/new-veeam-rce-flaw-lets-domain-users-hack-backup-servers/
4.https://www.veeam.com/kb4743
5.https://www.wordfence.com/blog/2025/06/attackers-actively-exploiting-critical-vulnerability-in-motors-theme/
6.https://www.securityweek.com/motors-theme-vulnerability-exploited-to-hack-wordpress-websites/
7.https://www.securityweek.com/motors-theme-vulnerability-exploited-to-hack-wordpress-websites/
8.https://www.securityweek.com/critical-authentication-bypass-flaw-patched-in-teleport/
9.https://support.goteleport.com/hc/en-us/articles/42280478593043-CVE-2025-49825-for-Cloud-Customers
10.https://www.securityweek.com/critical-vulnerability-exposes-many-mitel-micollab-instances-to-remote-hacking/
11.https://www.mitel.com/support/mitel-product-security-advisory-misa-2025-0007
12.https://karmainsecurity.com/dont-call-that-protected-method-vbulletin-rce
13.https://www.bleepingcomputer.com/news/security/hackers-are-exploiting-critical-flaw-in-vbulletin-forum-software/
14.https://securityaffairs.com/178481/security/two-flaws-in-vbulletin-forum-software-are-under-attack.html
15.https://horizon3.ai/attack-research/attack-blogs/cisco-ios-xe-wlc-arbitrary-file-upload-vulnerability-cve-2025-20188-analysis/
16.https://www.bleepingcomputer.com/news/security/exploit-details-for-max-severity-cisco-ios-xe-flaw-now-public/
17.https://www.bleepingcomputer.com/news/security/hewlett-packard-enterprise-warns-of-critical-storeonce-auth-bypass/
18.https://thehackernews.com/2025/06/critical-10-year-old-roundcube-webmail.html
19.https://fearsoff.org/research/roundcube
20.https://www.bleepingcomputer.com/news/security/hacker-selling-critical-roundcube-webmail-exploit-as-tech-info-disclosed/
21.https://www.bleepingcomputer.com/news/security/critical-fortinet-flaws-now-exploited-in-qilin-ransomware-attacks/
22.https://securityaffairs.com/178736/hacking/attackers-exploit-fortinet-flaws-to-deploy-qilin-ransomware.html
23.https://www.sentinelone.com/labs/follow-the-smoke-china-nexus-threat-actors-hammer-at-the-doors-of-top-tier-targets/
24.https://www.bleepingcomputer.com/news/security/sentinelone-shares-new-details-on-china-linked-breach-attempt/
25.https://thehackernews.com/2025/06/over-70-organizations-across-multiple.html
26.https://www.bankinfosecurity.com/sentinelone-sees-no-breach-after-hardware-supplier-hacked-a-28626
27.https://www.bankinfosecurity.com/sentinelone-sees-no-breach-after-hardware-supplier-hacked-a-28626
28.https://www.securityweek.com/chinese-espionage-crews-circle-sentinelone-in-year-long-reconnaissance-campaign/
29.https://www.theregister.com/2025/06/09/china_malware_flip_switch_sentinelone/
30.https://www.theregister.com/2025/06/09/china_malware_flip_switch_sentinelone/
31.https://reliaquest.com/blog/threat-spotlight-citrix-bleed-2-vulnerability-in-netscaler-adc-gateway-devices/
32.https://www.bleepingcomputer.com/news/security/citrix-bleed-2-flaw-now-believed-to-be-exploited-in-attacks/
33.https://www.darkreading.com/vulnerabilities-threats/citrixbleed-2-active-exploitation
34.https://www.infosecurity-magazine.com/news/citrixbleed-2-vulnerability/
35.https://www.securityweek.com/evidence-suggests-exploitation-of-citrixbleed-2-vulnerability/
36.
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/