[TLP: CLEAR]

Monthly Security Bulletin– March 2026

Overview

Greetings,

CERT Vanuatu, an operational unit of the Office of the Department of Communication and Digital Transformation, is pleased to present this Monthly Security Bulletin. This edition highlights key vulnerabilities and active exploits identified throughout March 2026 across widely used systems and applications. The bulletin is intended to serve as a valuable resource to support and strengthen your organization's cybersecurity preparedness.

Contacts

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

Threat Intelligence

Vulnerabilities and exploits

HPE Warns of Critical AOS-CX Flaw Allowing Admin Password Resets

"Hewlett Packard Enterprise (HPE) has patched multiple security vulnerabilities in the Aruba Networking AOS-CX operating system, including several authentication and code execution issues. AOS-CX is a cloud-native network operating system (NOS) developed by HPE subsidiary Aruba Networks for the company's CX-series campus and data center switch devices. The most severe security flaw today is a critical authentication bypass vulnerability (tracked as CVE-2026-23813) that attackers without privileges can

exploit in low-complexity attacks to reset admin passwords."
CERTVU recommends all users and organizations to read this vulnerability and follow the mitigation steps to mitigate these vulnerabilities.

https://www.bleepingcomputer.com/news/security/hpe-warns-of-critical-aos-cx-flaw-allowing-admin-password-resets/

SAP Patches Critical FS-QUO, NetWeaver Vulnerabilities
"Enterprise security firm SAP on Tuesday announced the release of 15 new security notes as part of its March 2026 Security Patch Day. The most important of these notes resolves critical-severity vulnerabilities in Quotation Management Insurance (FS-QUO) and NetWeaver Enterprise Portal Administration. SAP describes the FS-QUO bug, tracked as CVE-2019-17571 (CVSS score of 9.8), as a code injection issue."
CERTVU recommends all users and organizations to read this vulnerability and follow the mitigation steps to mitigate these vulnerabilities.

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

Critical Defect in Java Security Engine Poses Serious Downstream Security Risks
"A maximum-severity vulnerability in pac4j, an open-source library integrated into hundreds of software packages and repositories, poses a significant security threat, but has thus far received scant attention. The defect in the Java security engine, which handles authentication across multiple frameworks, has not been exploited in the wild since code review firm CodeAnt AI published a proof-of-concept exploit last week. The company discovered the vulnerability and privately reported it to pac4j's maintainer, which disclosed the defect and released patches for affected versions of the library within two days."
CERTVU recommends all users and organizations to read this advisory and follow the mitigation steps to mitigate these vulnerabilities.

https://cyberscoop.com/pac4j-open-source-library-vulnerability-max-severity-risk/

HPE Warns of Critical AOS-CX Flaw Allowing Admin Password Resets
"Hewlett Packard Enterprise (HPE) has patched multiple security vulnerabilities in the Aruba Networking AOS-CX operating system, including several authentication and code execution issues. AOS-CX is a cloud-native network operating system (NOS) developed by HPE subsidiary Aruba Networks for the company's CX-series campus and data center

switch devices. The most severe security flaw today is a critical authentication bypass vulnerability (tracked as CVE-2026-23813) that attackers without privileges can exploit in low-complexity attacks to reset admin passwords."
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/hpe-warns-of-critical-aos-cx-flaw-allowing-admin-password-resets/

SAP Patches Critical FS-QUO, NetWeaver Vulnerabilities
"Enterprise security firm SAP on Tuesday announced the release of 15 new security notes as part of its March 2026 Security Patch Day. The most important of these notes resolves critical-severity vulnerabilities in Quotation Management Insurance (FS-QUO) and NetWeaver Enterprise Portal Administration. SAP describes the FS-QUO bug, tracked as CVE-2019-17571 (CVSS score of 9.8), as a code injection issue."
CERTVU recommends all users and organizations to read this vulnerability and follow the mitigation steps to mitigate these vulnerabilities.

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

Critical Defect In Java Security Engine Poses Serious Downstream Security Risks
"A maximum-severity vulnerability in pac4j, an open-source library integrated into hundreds of software packages and repositories, poses a significant security threat, but has thus far received scant attention. The defect in the Java security engine, which handles authentication across multiple frameworks, has not been exploited in the wild since code review firm CodeAnt AI published a proof-of-concept exploit last week. The company discovered the vulnerability and privately reported it to pac4j's maintainer, which disclosed the defect and released patches for affected versions of the library within two days."
CERTVU recommends all users and organizations to read this Vulnerability and follow the mitigation steps to mitigate these vulnerabilities.

https://cyberscoop.com/pac4j-open-source-library-vulnerability-max-severity-risk/

Apeman Cameras
"Successful exploitation of these vulnerabilities could allow an attacker to take control of the device or view camera feeds."
CERTVU recommends all users and organizations to read this Vulnerability and follow the mitigation steps to mitigate these vulnerabilities.

https://www.cisa.gov/news-events/ics-advisories/icsa-26-069-01

Lantronix EDS3000PS And EDS5000

"Successful exploitation of these vulnerabilities could allow an attacker to bypass authentication and execute code with root-level privileges."

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

https://www.cisa.gov/news-events/ics-advisories/icsa-26-069-02

PTC Warns Of Imminent Threat From Critical Windchill, FlexPLM RCE Bu

"PTC Inc. is warning of a critical vulnerability in Windchill and FlexPLM, widely used product lifecycle management (PLM) solutions, that could allow remote code execution. The security issue, identified as CVE-2026-4681, could be leveraged through the deserialization of trusted data. Its severity has prompted emergency action from German authorities, with the federal police (BKA) reportedly sending agents to affected companies to alert them to the cybersecurity risk."

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

https://www.bleepingcomputer.com/news/security/ptc-warns-of-imminent-threat-from-critical-windchill-flexplm-rce-bug/

Oracle Pushes Emergency Fix For Critical Identity Manager RCE Flaw

"Oracle has released an out-of-band security update to fix a critical unauthenticated remote code execution vulnerability in Identity Manager and Web Services Manager tracked as CVE-2026-21992. Oracle Identity Manager is used for managing identities and access across an enterprise, while Oracle Web Services Manager provides security and management controls for web services. In an advisory released yesterday, Oracle is "strongly" recommending that customers apply the patches as soon as possible."

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

https://www.bleepingcomputer.com/news/security/oracle-pushes-emergency-fix-for-critical-identity-manager-rce-flaw/

Max Severity Ubiquiti UniFi Flaw May Allow Account Takeover

"Ubiquiti has patched two vulnerabilities in the UniFi Network Application, including a maximum-severity f law that may allow attackers to take over user accounts. The UniFi Network app (also known as the UniFi Controller) is management software that helps configure, monitor, and optimize Ubiquiti UniFi networking hardware, such as access points, switches, and gateways. "Combines powerful internet gateways with scalable WiFi and switching. Provides real-time traffic dashboards, visual topology maps, and optimization tips," the networking device manufacturer says. "The preferred way to deploy UniFi Network is on a UniFi Cloud Gateway, rather than on a server, laptop, or other self-hosted environment."

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

https://www.bleepingcomputer.com/news/security/ubiquiti-warns-of-unifi-flaw-that-may-enable-account-takeover/

Instant Hijack: Critical 10.0 CVSS File Browser Flaw Grants Automatic Admin Rights

"Security researchers have issued a high-priority alert for users of File Browser, a popular open-source self-hosted cloud storage solution. A critical logic flaw has been discovered in the platform's registration system that can automatically grant full administrative powers to any new user who signs up. The vulnerability, tracked as CVE-2026-32760, has been assigned a maximum CVSS score of 10, reflecting its potential for total system takeover with zero technical effort from an attacker."

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

https://securityonline.info/instant-hijack-critical-10-cvss-file-browser-flaw-cve-2026-32760/

Veeam Warns Of Critical Flaws Exposing Backup Servers To RCE Attacks

"Data protection company Veeam Software has patched multiple flaws in its Backup & Replication solution, including four critical remote code execution (RCE) vulnerabilities. VBR is enterprise data backup and recovery software that helps IT administrators to create copies of critical data for quick restoration following cyberattacks and hardware failures. Three RCE security flaws patched today (tracked as CVE-2026-21666, CVE-2026-21667, and CVE-2026-21669) allow low-privileged domain users to execute remote

code on vulnerable backup servers in low-complexity attacks."
CERTVU recommends all users and organizations to read this Vulnerability and follow the mitigation steps to mitigate these vulnerabilities.

https://www.bleepingcomputer.com/news/security/veeam-warns-of-critical-flaws-exposing-backup-servers-to-rce-attacks/

Malware

Trivy Under Attack Again: Widespread GitHub Actions Tag Compromise Exposes CI/CD Secrets
"A new supply chain attack targeting Trivy has been disclosed today by Paul McCarty, marking the second distinct compromise affecting the Trivy ecosystem in March. This latest incident impacts GitHub Actions, and is separate from the earlier OpenVSX compromise involving the VS Code extension. Initial reports have focused on the compromise of Trivy v0.69.4, with downstream ecosystems such as Homebrew already rolling back affected versions. The first known detection of suspicious activity traces back to approximately 19:15 UTC."

https://socket.dev/blog/trivy-under-attack-again-github-actions-compromise

Checkmarx KICS Code Scanner Targeted In Widening Supply Chain Hit
"Hard on the heels of a broad supply chain attack that impacted the Aqua Security-maintained Trivy open source security-scanner project, Checkmarx on Tuesday disclosed that attackers had compromised a version of Keeping Infrastructure as Code Secure (KICS), the open source static code analysis project that it develops and maintains. Specifically, the cybercriminals infiltrated KICS GitHub Action, which organizations use to run KICS scans within their CI/CD pipelines, and poisoned multiple versions of the software. Any organization that had its automated CI/CD pipelines configured to run the KICS GitHub Action during a four-hour window on the morning of March 23 could potentially be impacted, Checkmarx said."

https://www.darkreading.com/application-security/checkmarx-kics-code-scanner-widening-supply-chain

TeamPCP Isn't Done: Threat Actor Behind Trivy And KICS Compromises Now Hits LiteLLM's 95 Million Monthly Downloads On PyPI
"On March 24, 2026, Endor Labs identified that litellm versions 1.82.7 and 1.82.8 on PyPI contain malicious code not present in the upstream GitHub repository. litellm

is a widely used open source library with over 95 million month downloads. It lets developers route requests across LLM providers through a single API. Both compromised versions include a backdoored file that decodes and executes a hidden payload the moment the file is imported. Version 1.82.8 goes further: it installs a .pth file that runs the payload on any Python invocation, even if litellm is never imported. Version 1.82.6 is the last known-clean release."

https://www.endorlabs.com/learn/teampcp-isnt-done

Someone Has Publicly Leaked An Exploit Kit That Can Hack Millions Of iPhones

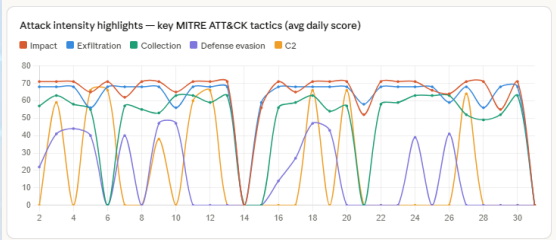
"Last week, cybersecurity researchers uncovered a hacking campaign targeting iPhone users that used an advanced hacking tool called DarkSword. Now someone has leaked a newer version of DarkSword and published it on the code-sharing site GitHub. Researchers are warning that this will allow any hacker to easily use the tools to target iPhone users running older versions of Apple's operating systems who have not yet updated to its latest iOS 26 software. This likely affects hundreds of millions of actively used iPhones and iPads, according to Apple's own data on out-of-date devices."

https://techcrunch.com/2026/03/23/someone-has-publicly-leaked-an-exploit-kit-that-can-hack-millions-of-iphones/

CERTVU Threat Statistics

Attack index summary

The month opened with an elevated but stable attack index in the mid-to-high 80s, then spiked sharply to a peak of 92.5 on March 7. From that point, there was a sustained and meaningful decline through the final two weeks of the month, bottoming at 72.6 on March 26 before a modest rebound to close at 80.3 on March 30. The overall trajectory — peak in the first third, gradual de-escalation — suggests a concentrated campaign or threat cluster early in the month that was progressively contained.

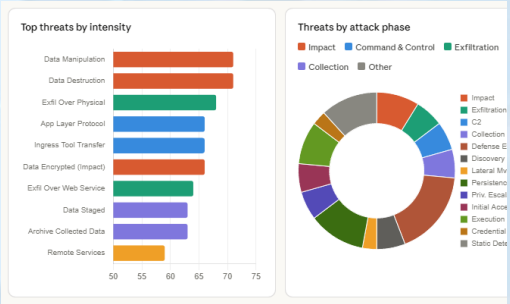


Source: CERTVU

Top Threats

The highest-intensity threats were concentrated in the Impact phase, with Data Manipulation (T1565) and Data Destruction (T1485) both scoring 71 — the maximum recorded for the period. These were closely followed by Exfiltration Over Physical Medium

(T1052) at intensity 68, indicating serious data loss risk. Application Layer Protocol (T1071) and Ingress Tool Transfer (T1105) scored 66, pointing to active Command & Control activity. Notably, a Data Encrypted for Impact (T1486) detection at intensity 66 suggests ransomware-related activity touching at least 2 devices.



Source: CERTVU

CERTVU Advisories

Advisory 120: Qualcomm Multiple Chipsets Memory Corruption Vulnerability

CVE-2026-21385 is a high-severity vulnerability (CVSS 7.8) affecting the graphics subsystem of certain Android devices that use Qualcomm chipsets. The flaw exists in the Qualcomm Adreno GPU graphics driver, which is responsible for handling graphics processing and memory allocation.

The vulnerability results from an integer overflow (CWE-190) during memory allocation calculations. When the system incorrectly calculates the required memory buffer size, it can lead to memory corruption, allowing data to overflow into restricted memory areas.

https://cert.gov.vu/index.php/advisories/116-advisory-120

Advisory 121: Apple iOS and iPadOS Use-After-Free Vulnerability

CVE-2023-41974 is a high-severity memory corruption vulnerability (CVSS 7.8) affecting Apple mobile operating systems. The flaw is classified as a Use-After-Free (CWE-416) vulnerability in the system's kernel memory management.

A use-after-free vulnerability occurs when a program continues to use a memory pointer after the memory has already been freed. This can lead to memory corruption, allowing attackers to manipulate system memory and potentially execute malicious code.

https://cert.gov.vu/index.php/advisories/117-advisory-121

Advisory 122: SolarWinds Web Help Desk Deserialization of Untrusted Data Vulnerability

CVE-2025-26399 is a critical remote code execution (RCE) vulnerability affecting the SolarWinds Web Help Desk platform. The vulnerability arises from deserialization of untrusted data (CWE-502) in the AjaxProxy component, which fails to properly validate user-supplied input before processing it.

https://cert.gov.vu/index.php/advisories/118-advisory-122

Advisory 123: Ivanti Endpoint Manager (EPM) Authentication Bypass Vulnerability

CVE-2026-1603 is a high-severity authentication bypass vulnerability affecting enterprise endpoint management software. The flaw exists in Ivanti Endpoint Manager (EPM) and allows a remote, unauthenticated attacker to bypass authentication controls and access sensitive stored credentials within the system.

The vulnerability results from improper authentication handling (CWE-288 / CWE-306) in the application. Specifically, certain internal API endpoints do not correctly enforce authentication checks, allowing attackers to access protected resources through alternative request paths.

https://cert.gov.vu/index.php/advisories/119-advisory-123

Advisory 124: Microsoft SharePoint Deserialization of Untrusted Data Vulnerability

CVE-2026-1603 is a high-severity authentication bypass vulnerability affecting enterprise endpoint management software. The flaw exists in Ivanti Endpoint Manager (EPM) and allows a remote, unauthenticated attacker to bypass authentication controls and access sensitive stored credentials within the system.

https://cert.gov.vu/index.php/advisories/121-advisory-124

Upcoming Events

Digital Week – Vanuatu

Digital Week Vanuatu is a national event that brings together government, businesses, innovators, and communities to celebrate and advance the country's digital transformation. Evolving from the long-running National ICT Days, it combines key activities like e-commerce discussions, innovation showcases, and public engagement events into a dynamic, multi-day program focused on technology, inclusion, and sustainable development.

The 2026 Cyber security Boot Camp

As part of Digital Week Vanuatu, a Cybersecurity Boot Camp is organized each year to inspire and equip young people with essential digital safety and cybersecurity skills. Supported by CERT Vanuatu (CERTVU) and the Department of Communication and Digital Transformation, the initiative targets senior secondary school students through hands-on learning experiences that raise awareness of online threats and introduce core cybersecurity concepts.

The program is designed to help develop the next generation of cybersecurity professionals in Vanuatu by combining interactive sessions, practical exercises, and discussions on responsible internet use and the protection of digital

information. Participants are also recognized for their involvement, helping to build confidence and encourage interest in careers within the expanding ICT and cybersecurity sectors.

Cyber month Event

October has been designated as Cyber Month; a time focused on strengthening cybersecurity efforts nationwide. As part of the Cyber Up Pacific initiative, the CERTVU (CERT Vanuatu) team will spearhead a series of Cyber Week activities aimed at increasing cybersecurity awareness among communities, educational institutions, and both public and private sector organizations.

Through these initiatives, the public will be equipped with practical knowledge on safe online practices, supporting Vanuatu's ongoing efforts to build a more secure and resilient digital environment while contributing to the broader protection of the region's digital landscape.

CERT Vanuatu Efforts

CERT Vanuatu (CERT-VU) continues to play a vital role in strengthening cybersecurity across the country. By working closely with a broad range of stakeholders, CERT-VU addresses emerging cyber threats and challenges, helping to build a digitally aware community that is better prepared and more resilient against cyberattacks.

Cybersecurity Awareness Program

CERTVU continues to implement a variety of initiatives under its ongoing cybersecurity awareness program.

Digital Road Show 2026

An awareness was made during the digital road show 2026 in Emua village and at Melemat Village.

Source: CERTVU

Famili I ready Program

As part of ongoing awareness for the Famili I Ready program, CERTVU conducted an awareness session during a workshop held at the Cultural Center from March 16 to 20, 2026.

In addition, CERTVU utilizes digital platforms to share cybersecurity awareness materials with the wider public.

Its presence on Facebook serves as a key communication channel, enabling broader outreach and encouraging engagement and discussions on cybersecurity and related issues.

Multi-stakeholder Initiative

Cloud infrastructure Roadmap and Cyber Security Agency

The Department of Communication and Digital Transformation (DCDT) is actively working with national stakeholders on two key initiatives: the development of a Cloud Infrastructure Roadmap and the establishment of a dedicated Cybersecurity Agency.

The Cloud Infrastructure Roadmap aims to provide clear strategic guidance for adopting cloud technologies across government systems and public services. Through close collaboration with local partners, DCDT is ensuring the roadmap reflects Vanuatu's unique needs and capacities, supporting a smooth and effective transition to cloud-based solutions.

At the same time, progress is being made toward establishing a Cybersecurity Agency, which will serve as a central authority for strengthening the country's cybersecurity framework. This agency is expected to provide coordinated oversight, develop national policies, and collaborate across sectors to protect critical digital assets and address emerging cyber threats. Together, these initiatives highlight the Government of Vanuatu's commitment to strengthening digital infrastructure and enhancing cybersecurity readiness, contributing to a more secure and resilient digital future.

International Collaboration

CERT Vanuatu (CERT-VU) continues to demonstrate its commitment to strengthening and sustaining international partnerships, reinforcing its presence and contribution within the global cybersecurity landscape.

PACSON

The Department of Communication and Digital Transformation (DCDT), through CERTVU, actively participates in several key working groups under the Pacific Cyber Security Operational Network (PACSON).

- **Awareness Raising Working Group:** This group focuses on promoting cybersecurity awareness across the Pacific. A key initiative is the Cybersmart awareness materials, which help educate individuals and organizations on online risks and safe digital practices.
- **Community Working Group:** This group works to build a strong and resilient cybersecurity community by encouraging best practices and facilitating information sharing among Pacific countries.
- **Capacity Building Working Group:** This group aims to strengthen regional cybersecurity capabilities by delivering targeted training and support to address knowledge gaps and enhance technical skills.

Through its engagement in these working groups, DCDT, through CERTVU, continues to contribute to a safer and more resilient digital environment across the Pacific region.

Incident Response

CERTVU operates a dedicated incident response team that actively monitors and manages emerging cyber threats daily.

This team is essential in identifying, assessing, and responding to incidents, helping to reduce risks and protect both individuals and organizations from potential harm. Through continuous monitoring, capacity development, and awareness efforts, CERTVU works to limit the impact of cyber threats and enhance national readiness. These efforts underscore the importance of strong coordination and resilience in ensuring a secure digital environment.

References

1. https://www.bleepingcomputer.com/news/security/veeam-warns-of-critical-flaws-exposing-backup-servers-to-rce-attacks/
2. https://www.veeam.com/kb4830
3. https://www.bleepingcomputer.com/news/security/oracle-pushes-emergency-fix-for-critical-identity-manager-rce-flaw/
4. https://www.oracle.com/security-alerts/alert-cve-2026-21992.html
5. https://www.darkreading.com/vulnerabilities-threats/patch-oracle-fusion-middleware-rce-flaw
7. https://thehackernews.com/2026/03/oracle-patches-critical-cve-2026-21992.html
8. https://securityaffairs.com/189796/security/oracle-fixes-critical-rce-flaw-cve-2026-21992-in-identity-manager.html
9. https://www.bleepingcomputer.com/news/security/ubiquiti-warns-of-unifi-flaw-that-may-enable-account-takeover/
10. https://community.ui.com/releases/Security-Advisory-Bulletin-062-062/c29719c0-405e-4d4a-8f26-e343e99f931b
11. https://securityaffairs.com/189689/security/critical-ubiquiti-unifi-unifi-security-flaw-allows-potential-account-hijacking.html
12. https://www.bleepingcomputer.com/news/security/ptc-warns-of-imminent-threat-from-critical-windchill-flexplm-rce-bug/
13. https://www.ptc.com/en/about/trust-center/advisory-center/active-advisories/windchill-flexplm-critical-vulnerability
14. https://www.heise.de/en/news/WTF-Police-responded-on-Saturday-night-due-to-a-zero-day-11221590.html
15. https://www.bleepingcomputer.com/news/security/hpe-warns-of-critical-aos-cx-flaw-allowing-admin-password-resets/
16. https://www.securityweek.com/sap-patches-critical-fs-quo-netweaver-vulnerabilities/
17. https://cyberscoop.com/pac4j-open-source-library-vulnerability-max-severity-risk/
18. https://www.bleepingcomputer.com/news/security/hpe-warns-of-critical-aos-cx-flaw-allowing-admin-password-resets/
19. https://www.securityweek.com/sap-patches-critical-fs-quo-netweaver-vulnerabilities/
20. https://cyberscoop.com/pac4j-open-source-library-vulnerability-max-severity-risk/
21. https://socket.dev/blog/trivy-under-attack-again-github-actions-compromise
22. https://github.com/aquasecurity/trivy/discussions/10425
23. https://www.wiz.io/blog/trivy-compromised-teampcp-supply-chain-attack
24. https://www.aikido.dev/blog/teampcp-deploys-worm-npm-trivy-compromise
25. https://thehackernews.com/2026/03/trivy-security-scanner-github-actions.html
26. https://thehackernews.com/2026/03/trivy-supply-chain-attack-triggers-self.html
27. https://www.bleepingcomputer.com/news/security/trivy-vulnerability-scanner-breach-pushed-infostealer-via-github-actions/

 © CERTVU 2026

28. https://www.darkreading.com/application-security/checkmarx-kics-code-scanner-widening-supply-chain
29. https://checkmarx.com/blog/checkmarx-security-update/
30. https://thehackernews.com/2026/03/teampcp-hacks-checkmarx-github-actions.html
31. https://www.endorlabs.com/learn/teampcp-isnt-done
32. https://www.bleepingcomputer.com/news/security/popular-litellm-pypi-package-compromised-in-teampcp-supply-chainattack/
33. https://thehackernews.com/2026/03/teampcp-backdoors-litellm-versions.html
34. https://www.theregister.com/2026/03/24/trivy_compromise_litellm/
35. https://techcrunch.com/2026/03/23/someone-has-publicly-leaked-an-exploit-kit-that-can-hack-millions-of-iphones/
36. https://cyberscoop.com/darksword-iphone-spyware-leak-ios-18-exploit-threat/
37. https://hackread.com/darksword-iphone-exploit-leaked-online/
38. https://cert.gov.vu/
39. https://www.cto.int/event-details/the-commonwealth-digital-roadshow-vanuatu
40. https://www.facebook.com/CERTVU