[TLP: CLEAR]

Monthly Security Bulletin– February 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 February 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

n8n Sandbox Escape: Critical Vulnerabilities In n8n Exposes Hundreds Of Thousands Of Enterprise AI Systems To Complete Takeover

"Pillar Security researchers uncovered critical vulnerabilities in n8n, a popular open-source workflow automation platform powering numerous enterprise deployments. The vulnerabilities allowed any authenticated user to seize complete control of the server, stealing every stored credential, API key, and secret on both self-hosted and cloud instances. On n8n Cloud, the shared multi-tenant architecture meant a single malicious user could

potentially breach the entire platform, accessing data belonging to all other customers."
CERTVU recommends all users and organizations to read this vulnerability and follow the mitigation steps to mitigate these vulnerabilities.

https://www.pillar.security/blog/n8n-sandbox-escape-critical-vulnerabilities-in-n8n-exposes-hundreds-of-thousands-of-enterprise-ai-systems-to-complete-takeover

Trend Micro Patches Critical Apex One Vulnerabilities
"TrendAI, the new name of Trend Micro's enterprise business, on Wednesday announced patches for several critical and high-severity vulnerabilities found in the Windows and macOS versions of the Apex One endpoint security solution. A total of eight vulnerabilities have been addressed, including two with a critical severity rating based on their CVSS scores. The critical flaws both impact the Trend Micro Apex One management console and "could allow a remote attacker to upload malicious code and execute commands on affected installations"

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

https://www.securityweek.com/trend-micro-patches-critical-apex-one-vulnerabilities/

Critical Juniper Networks PTX Flaw Allows Full Router Takeover
"A critical vulnerability in the Junos OS Evolved network operating system running on PTX Series routers from Juniper Networks could allow an unauthenticated attacker to execute code remotely with root privileges. PTX Series routers are high-performance core and peering routers built for high throughput, low latency, and scale. They are commonly used by internet service providers, telecommunication services, and cloud network applications. The security issue is identified as CVE-2026-21902 and is caused by incorrect permission assignment in the 'On-Box Anomaly Detection' framework, which should be exposed to internal processes only over the internal routing interface."
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-juniper-networks-ptx-flaw-allows-full-router-takeover/

Critical Cisco SD-WAN Bug Exploited In Zero-Day Attacks Since 2023 1/

"Cisco is warning that a critical authentication bypass vulnerability in Cisco Catalyst SD-WAN, tracked as CVE-2026-20127, was actively exploited in zero-day attacks that allowed remote attackers to compromise controllers and add malicious rogue peers to targeted networks. CVE-2026-20127 has a maximum severity of 10.0 and impacts Cisco Catalyst SD-WAN Controller (formerly vSmart) and Cisco Catalyst SD-WAN Manager (formerly vManage) in on-prem and SD-WAN Cloud installations. Cisco credited the Australian Signals Directorate's Australian Cyber Security Centre (ASD's ACSC) for reporting the vulnerability."

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-sd-wan-bug-exploited-in-zero-day-attacks-since-2023/

From PDF To Pwn: Scalable 0day Discovery In PDF Engines And Services Using Multi-Agent LLMs

"When preparing to emerge from stealth, we sought to demonstrate the efficacy of our research workflow by targeting Apryse WebViewer (formerly PDFTron) and Foxit PDF cloud services. These platforms are widely deployed, feature-rich, and combine client-side UI logic with complex server-side SDKs, making them an ideal proving ground for vulnerability research. Our strategy involved a human agent symbiosis: our researchers manually identified foundational vulnerability patterns, which were then taught to the Novee agent. Once the agent internalized the “scent” of these bugs, it autonomously explored the massive attack surface of both vendors. The result was the discovery of 13 distinct vulnerability categories, ranging from critical XSS to OS Command Injection."

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

https://novee.security/blog/from-pdf-to-pwn-scalable-0day-discovery-in-pdf-engines-and-services-using-multi-agent-llms-2/

From BRICKSTORM To GRIMBOLT: UNC6201 Exploiting a Dell RecoverPoint For Virtual Machines Zero-Day

"Mandiant and Google Threat Intelligence Group (GTIG) have identified the zero-day exploitation of a high-risk vulnerability in Dell RecoverPoint for Virtual Machines, tracked as CVE-2026-22769, with a

CVSSv3.1 score of 10.0. Analysis of incident response engagements revealed that UNC6201, a suspected PRC-nexus threat cluster, has exploited this flaw since at least mid-2024 to move laterally, maintain persistent access, and deploy malware including SLAYSTYLE, BRICKSTORM, and a novel backdoor tracked as GRIMBOLT. The initial access vector for these incidents was not confirmed, but UNC6201 is known to target edge appliances (such as VPN concentrators) for initial access. There are notable overlaps between UNC6201 and UNC5221, which has been used synonymously with the actor publicly reported as Silk Typhoon, although GTIG does not currently consider the two clusters to be the same."
CERTVU recommends all users and organizations to read this Vulnerability and follow the mitigation steps to mitigate these vulnerabilities.

https://cloud.google.com/blog/topics/threat-intelligence/unc6201-exploiting-dell-recoverpoint-zero-day/

800,000 WordPress Sites Affected By Arbitrary File Upload Vulnerability In WPvivid Backup WordPress Plugin

"On January 12th, 2026, we received a submission for an Arbitrary File Upload vulnerability in WPvivid Backup, a WordPress plugin with more than 800,000 active installations. This vulnerability can be used by unauthenticated attackers to upload arbitrary files to a vulnerable site and achieve remote code execution, which is typically leveraged for a complete site takeover. Please note that this vulnerability only critically affects users who have a generated key in the plugin settings to allow another site to send a backup to their site. This feature is disabled by default, and the key expiration can only be set to a maximum of 24 hours."
CERTVU recommends all users and organizations to read this Vulnerability and follow the mitigation steps to mitigate these vulnerabilities.

https://www.wordfence.com/blog/2026/02/800000-wordpress-sites-affected-by-arbitrary-file-upload-vulnerability-in-wpvivid-backup-wordpress-plugin/

SAP Patches Critical CRM, S/4HANA, NetWeaver Vulnerabilities

"SAP on Tuesday announced the release of 27 new and updated security notes, including two that address critical-severity vulnerabilities. The first critical security note released on SAP's February 2026 security patch day addresses CVE-2026-0488 (CVSS score of 9.9), a code injection bug in CRM and S/4HANA. Impacting the Scripting Editor component of the

applications, the flaw can be exploited by authenticated attackers to execute arbitrary SQL statements."
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-crm-s-4hana-netweaver-vulnerabilities/

BeyondTrust Warns Of Critical RCE Flaw In Remote Support Software
"BeyondTrust warned customers to patch a critical security flaw in its Remote Support (RS) and Privileged Remote Access (PRA) software that could allow unauthenticated attackers to execute arbitrary code remotely. Tracked as CVE-2026-1731, this pre-authentication remote code execution vulnerability stems from an OS command injection weakness discovered by Harsh Jaiswal and the Hacktron AI team, and it affects BeyondTrust Remote Support 25.3.1 or earlier and Privileged Remote Access 24.3.4 or earlier. Threat actors with no privileges can exploit it through maliciously crafted client requests in low-complexity attacks that don't require user interaction."
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/beyondtrust-warns-of-critical-rce-flaw-in-remote-support-software/

Claude Desktop Extensions Exposes Over 10,000 Users To Remote Code Execution Vulnerability
"LayerX discovered a zero-click remote code execution (RCE) vulnerability in Claude Desktop Extensions (DXT), in which a single Google Calendar event can silently compromise a system running Claude Desktop Extensions. The flaw impacts more than 10,000 active users and 50 DXT extensions. Unlike traditional browser extensions, Claude Desktop Extensions run unsandboxed with full system privileges. As a result, Claude can autonomously chain low-risk connectors (e.g., Google Calendar) to high-risk local executors, without user awareness or consent. If exploited by a bad actor, even a benign prompt (“take care of it”), coupled with a maliciously worded calendar event, is sufficient to trigger arbitrary local code execution that compromises the entire system."
CERTVU recommends all users and organizations to read this Vulnerability and follow the mitigation steps to mitigate these vulnerabilities.

https://www.infosecurity-magazine.com/news/zeroclick-flaw-claude-dxt/

Malware

CISA: VMware ESXi Flaw Now Exploited In Ransomware Attacks
"CISA confirmed on Wednesday that ransomware gangs have begun exploiting a high-severity VMware ESXi sandbox escape vulnerability that was previously used in zero-day attacks. Broadcom patched this ESXi arbitrary-write vulnerability (tracked as CVE-2025-22225) in March 2025 alongside a memory leak (CVE-2025-22226) and a TOCTOU flaw (CVE-2025-22224), and tagged them all as actively exploited zero-days. "A malicious actor with privileges within the VMX process may trigger an arbitrary kernel write leading to an escape of the sandbox," Broadcom said about the CVE-2025-22225 flaw."

https://www.bleepingcomputer.com/news/security/cisa-vmware-esxi-flaw-now-exploited-in-ransomware-attacks/

Hackers Compromise NGINX Servers To Redirect User Traffic
"A threat actor is compromising NGINX servers in a campaign that hijacks user traffic and reroutes it through the attacker's backend infrastructure. NGINX is open-source software for web traffic management. It intermediates connections between users and servers and is employed for web serving, load balancing, caching, and reverse proxying. The malicious campaign, discovered by researchers at DataDog Security Labs, targets NGINX installations and Baota hosting management panels used by sites with Asian top-level domains (.in, .id, .pe, .bd, and .th) and government and educational sites (.edu and .gov)."

https://www.bleepingcomputer.com/news/security/hackers-compromise-nginx-servers-to-redirect-user-traffic/

Google Ads And Claude AI Abused To Spread MacSync Malware Via ClickFix
"Cyber security researchers at Moonlock Lab, the investigative unit of the popular software developer MacPaw, have uncovered a clever new way that hackers are targeting Mac users. This campaign uses the ClickFix technique, where people are tricked into copying and pasting dangerous commands directly into their computer's Terminal and the attack starts with a simple Google search."

https://hackread.com/google-ads-claude-ai-macsync-malware-clickfix/

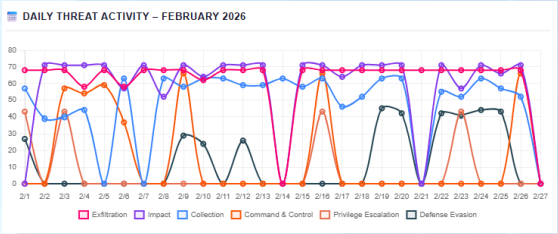
LockBit Strikes With New 5.0 Version, Targeting Windows, Linux And ESXI System

"In September 2025, a new version of LockBit ransomware was released, supporting Windows, Linux and ESXi systems, with a primary target being the U.S. business sector. As is typical for the ransomware-as-a-service model, LockBit employs a double-extortion scheme, also exfiltrating files to the attacker's server to increase the likelihood of receiving the ransom. As threat actors advertised, this version has improved defense evasion and fast encryption, and having multiple systems support makes this malware a very serious threat. What's notable among the multiple systems support its proclaimed capability to "work on all versions of Proxmox." Proxmox is an open-source virtualization platform and is being adopted by enterprises as an alternative to commercial hypervisors, which makes it another prime target of ransomware attacks."

https://www.acronis.com/en/tru/posts/lockbit-strikes-with-new-50-version-targeting-windows-linux-and-esxi-systems/

CERTVU Threat Statistics

During February 2026, the CERT Vanuatu threat monitoring platform recorded a total of 5938 risk event scores across 26 active threat days out of the 27-day reporting period, with only a handful of quiet days showing no detectable activity.

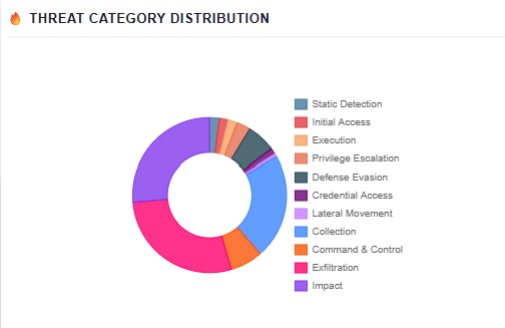


Source: CERVTU

The most persistently active threat categories were Exfiltration (cumulative score: 1674) and Impact (1567), both of which were flagged on a near-daily basis, indicating sustained attempts to extract data and cause operational disruption throughout the month. Collection (1295) and Command & Control (405) activity remained consistently elevated, suggesting active attacker infrastructure maintaining footholds and aggregating data ahead of exfiltration operations. Notable spikes were observed during the weeks of 3–6 February and 22–26 February, with Privilege Escalation, Defense Evasion, and Initial Access tactics recorded on multiple days — pointing to coordinated, multi-stage intrusion attempts aligned with the MITRE ATT&CK framework.

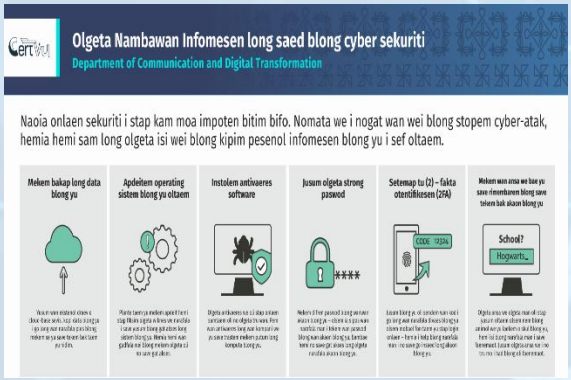
Encouragingly, Persistence, Discovery, and Lateral Movement tactics recorded minimal or zero scores across the

month, suggesting that while threat actors are active at the access and impact stages, deep network entrenchment has so far been limited. CERT Vanuatu recommends immediate prioritization of exfiltration controls and C2 traffic blocking, a review of privilege escalation vectors, and continued monitoring throughout March 2026 given the sustained elevated risk posture observed this period.



Source: CERTVU

Best Practice and Tips



Source:CERTVU/ file:///C:/Users/Jmalwerssets/Downloads/Top%20Tips_Bislama.pdf

Upcoming Events

Commonwealth Digital Roadshow – Vanuatu

The Commonwealth Telecommunications Organisation (CTO), in partnership with the Government of Vanuatu's Department of Communications and Digital Transformation, proudly presents the Commonwealth Digital Roadshow in Vanuatu—a three-day event dedicated to accelerating the nation's digital transformation journey.

This initiative brings together government leaders, industry experts, community representatives, and international partners to build momentum toward an inclusive and resilient digital future.

The Roadshow aims to inspire, educate, and connect stakeholders across Vanuatu, showcasing how digital technologies can drive sustainable development, economic growth, and improved public services.

Source: DCDT [The Commonwealth Digital Roadshow - Vanuatu | CTO Live site]

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

The continued efforts of CERT Vanuatu (CERT-VU) to strengthen cybersecurity across the country remain critically important. Through close collaboration with a wide range of stakeholders, CERT-VU addresses emerging cyber threats and challenges, working 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. A central component of this outreach includes regular participation in Radio Vanuatu's morning programs, where interactive ICT discussions are delivered to inform, educate, and engage the public on key digital topics.

Source: CERTVU

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 collaborating 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 is intended to provide strategic direction for the adoption of cloud technologies across government systems and public services. Through close engagement with local partners, the DCDT aims to ensure that the roadmap is aligned with Vanuatu's specific needs and capacities, enabling a smooth and effective transition to cloud-based solutions.

At the same time, work is progressing toward the creation of a Cybersecurity Agency, which will serve as a central authority for strengthening the country's cybersecurity framework. The agency is expected to provide coordinated oversight, develop national policies, and work across sectors to safeguard critical digital assets and respond to emerging cyber threats.

Together, these initiatives demonstrate the Government of Vanuatu's commitment to enhancing its digital infrastructure and cybersecurity readiness, supporting a more secure and resilient digital future for the nation.

Capacity Building Program

The Cybersecurity Training and Exercise Program for Pacific Islands and Territories was successfully held in Suva from 2nd to 5th February 2026, bringing together cybersecurity professionals and government representatives from across the Pacific region.

The program was supported by the Japan International Cooperation Agency (JICA) and Japan's Ministry of Internal Affairs and Communications (MIC), in collaboration with the Fiji Police Force.

The training focused on strengthening national incident response capabilities, enhancing regional coordination, and improving preparedness to respond to emerging cyber threats. Participants took part in practical exercises and scenario-based simulations designed to test real-world cyber incident response and inter-agency cooperation.

Vanuatu's participation reflects its strong commitment to building national cyber resilience and strengthening partnerships across the Pacific to better prevent, detect, and respond to cybersecurity threats.

Source: CERTVU

Trend Micro Training

The Advance Malware Analysis Training was successfully held in Suva from 16th to 20th February 2026, delivered by Trend Micro.

The intensive five-day training brought together cybersecurity professionals to strengthen technical skills in malware detection, reverse engineering, threat analysis, and incident response. Participants gained hands-on experience in analysing malicious code, understanding attacker techniques, and applying advanced investigation methodologies.

Five participants from the Department of Communications and Digital Transformation (DCDT) proudly represented Vanuatu, enhancing national capacity to respond to increasingly sophisticated cyber threats.

This training marks another important step in strengthening Vanuatu's cybersecurity capabilities and building technical expertise to better protect government systems and critical information infrastructure.

International Collaboration

CERT Vanuatu (CERT-VU) has been Steadfast in maintaining and strengthening its international collaborations over the years to elevate its position in the global cybersecurity landscape.

PACSON

The Department of Digital Communication and Digital Transformation (DCDT) through CERTVU, plays a continuous role in several key working groups within the Pacific Cyber Security Operational Network (PACSON).

- **Awareness Raising Working Group**: This group focuses on spreading cybersecurity knowledge across the Pacific. One of its key initiatives is the **Cybersmart** awareness materials, which are used to educate the public and organizations about online threats and safe practices.
- **Community Working Group**: This group aims to create a cohesive and resilient cyber community by promoting best practices and facilitating information sharing among Pacific nations.
- **Capacity Building Working Group**: This group is dedicated to enhancing the region's cybersecurity capabilities by providing targeted training and support to fill knowledge gaps and strengthen skills.

Through its involvement in these groups, DCDT, via CERTVU, is actively contributing to a stronger, more secure digital environment across the Pacific.

Incident Response

CERTVU maintains a proactive incident response team dedicated to the continuous monitoring and management of emerging cyber threats on a daily basis. The team plays a vital role in detecting, analyzing, and mitigating incidents, helping to prevent potential disruptions and safeguard both individuals and organizations. Through sustained efforts in monitoring, capacity building, and awareness initiatives, CERTVU works to minimize the impact of cyber threats and strengthen national preparedness. These actions highlight the importance of resilience and coordinated response in maintaining a secure digital environment.

References

1. https://www.pillar.security/blog/n8n-sandbox-escape-critical-vulnerabilities-in-n8n-exposes-hundreds-of-thousands-of-enterprise-ai-systems-to-complete-takeover
2. https://www.bleepingcomputer.com/news/security/critical-n8n-flaws-disclosed-along-with-public-exploits/
3. https://www.infosecurity-magazine.com/news/two-critical-flaws-in-n8n-ai/
4. https://www.securityweek.com/trend-micro-patches-critical-apex-one-vulnerabilities/
5. https://success.trendmicro.com/en-US/solution/KA-0022458
7. https://www.bleepingcomputer.com/news/security/trend-micro-warns-of-critical-apex-one-rce-vulnerabilities/
8. https://securityaffairs.com/188572/security/trend-micro-fixes-two-critical-flaws-in-apex-one.html
9. https://www.bleepingcomputer.com/news/security/critical-juniper-networks-ptx-flaw-allows-full-router-takeover/
10. https://supportportal.juniper.net/s/article/2026-02-Out-of-Cycle-Security-Bulletin-Junos-OS-Evolved-PTX-Series-A-vulnerability-allows-a-unauthenticated-network-based-attacker-to-execute-code-as-root-CVE-2026-21902
11. https://www.bleepingcomputer.com/news/security/critical-cisco-sd-wan-bug-exploited-in-zero-day-attacks-since-2023/
12. https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sdwan-rpa-EHchtZk
13. https://blog.talosintelligence.com/uat-8616-sd-wan/
14. https://www.cisa.gov/news-events/alerts/2026/02/25/cisa-and-partners-release-guidance-ongoing-global-exploitation-cisco-sd-wan-systems
15. https://cyberscoop.com/cisco-zero-days-cisa-emergency-directive-five-eyes/
16. https://www.helpnetsecurity.com/2026/02/25/cisco-sd-wan-zero-day-cve-2026-20127/
17. https://www.bleepingcomputer.com/news/security/critical-cisco-sd-wan-bug-exploited-in-zero-day-attacks-since-2023/
18. https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sdwan-rpa-EHchtZk
19. https://blog.talosintelligence.com/uat-8616-sd-wan/
20. https://www.cisa.gov/news-events/alerts/2026/02/25/cisa-and-partners-release-guidance-ongoing-global-exploitation-ciscosd-wan-systems
21. https://cyberscoop.com/cisco-zero-days-cisa-emergency-directive-five-eyes/
22. https://www.helpnetsecurity.com/2026/02/25/cisco-sd-wan-zero-day-cve-2026-20127/
23. https://novee.security/blog/from-pdf-to-pwn-scalable-0day-discovery-in-pdf-engines-and-services-using-multi-agent-llms-2/
24. https://www.securityweek.com/vulnerabilities-in-popular-pdf-platforms-allowed-account-takeover-data-exfiltration/

25. https://cloud.google.com/blog/topics/threat-intelligence/unc6201-exploiting-dell-recoverpoint-zero-day/
26. https://www.wordfence.com/blog/2026/02/800000-wordpress-sites-affected-by-arbitrary-file-upload-vulnerability-in-wpvivid-backup-wordpress-plugin/
27. https://www.securityweek.com/sap-patches-critical-crm-s-4hana-netweaver-vulnerabilities/
28. https://www.infosecurity-magazine.com/news/zeroclick-flaw-claude-dxt/
29. https://www.bleepingcomputer.com/news/security/beyondtrust-warns-of-critical-rce-flaw-in-remote-support-software/
30. https://www.bleepingcomputer.com/news/security/cisa-vmware-esxi-flaw-now-exploited-in-ransomware-attacks/
31. https://securityaffairs.com/187637/security/cve-2025-22225-in-vmware-esxi-now-used-in-active-ransomware-attacks.html
32. https://www.bleepingcomputer.com/news/security/cisa-vmware-esxi-flaw-now-exploited-in-ransomware-attacks/
33. https://securityaffairs.com/187637/security/cve-2025-22225-in-vmware-esxi-now-used-in-active-ransomware-attacks.html
34. https://www.bleepingcomputer.com/news/security/hackers-compromise-nginx-servers-to-redirect-user-traffic/
35. https://www.acronis.com/en/tru/posts/lockbit-strikes-with-new-50-version-targeting-windows-linux-and-esxi-systems/
36. https://www.helpnetsecurity.com/2026/02/16/lockbit-5-0-ransomware-windows-linux-esxi/
37. https://hackread.com/google-ads-claude-ai-macsync-malware-clickfix/
38. *file:///C:/Users/Jmalwerssets/Downloads/Top%20Tips_Bislama.pdf*
39. https://www.cto.int/event-details/the-commonwealth-digital-roadshow-vanuatu