[TLP: CLEAR]

Monthly Security Bulletin– April 2026

Overview

Greetings,

CERT Vanuatu, operating under the Office of the Department of Communication and Digital Transformation, is pleased to share this Monthly Security Bulletin. This edition provides an overview of significant vulnerabilities and active exploits identified during April 2026 across commonly used systems and applications. It is designed to support your organization in enhancing its cybersecurity awareness and overall 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

Vulnerabilities Patched In CrowdStrike, Tenable Products

"CrowdStrike and Tenable informed customers this week about potentially serious vulnerabilities found and patched in their products. CrowdStrike published an advisory for CVE-2026-40050, a critical unauthenticated path traversal vulnerability affecting its LogScale product. The flaw can allow a remote attacker to read arbitrary files from the server filesystem. The cybersecurity giant pointed out that Next-Gen SIEM customers are not affected and the vulnerability has been mitigated for LogScale SaaS customers. LogScale Self-hosted customers have been advised to update to a patched version."

CERTVU recommends all users and organizations to read this vulnerability and follow the

mitigation steps to mitigate these vulnerabilities.

https://www.securityweek.com/vulnerabilities-patched-in-crowdstrike-tenable-products/

Breeze Cache <= 2.4.4 - Unauthenticated Arbitrary File Upload Via Fetch_gravatar_from_remote

"The Breeze Cache plugin for WordPress is vulnerable to arbitrary file uploads due to missing file type validation in the 'fetch_gravatar_from_remote' function in all versions up to, and including, 2.4.4. This makes it possible for unauthenticated attackers to upload arbitrary files on the affected site's server which may make remote code execution possible. The vulnerability can only be exploited if "Host Files Locally - Gravatars" is enabled, which is disabled by default."
CERTVU recommends all users and organizations to read this vulnerability and follow the mitigation steps to mitigate these vulnerabilities.

https://www.wordfence.com/threat-ntel/vulnerabilities/wordpress-plugins/breeze/breeze-cache-244-unauthenticatedarbitrary-file-upload-via-fetch-gravatar-from-remote

SGLang Is Vulnerable To Remote Code Execution When Rendering Chat Templates From a Model File

"A remote code execution vulnerability has been discovered in the SGLang project, specifically in the reranking endpoint (/v1/rerank). A CVE has been assigned to track the vulnerability; CVE-2026-5760. An attacker can create a malicious model for SGLang to achieve RCE. Successful exploitation could allow arbitrary code execution in the context of the SGLang service, potentially leading to host compromise, lateral movement, data exfiltration, or denial-of-service (DoS) attacks. No response was obtained from the project maintainers during coordination."
CERTVU recommends all users and organizations to read this advisory and follow the mitigation steps to mitigate these vulnerabilities.

https://thehackernews.com/2026/04/sglang-cve-2026-5760-cvss-98-enables.html

Cisco Patches Four Critical Identity Services, Webex Flaws Enabling Code Execution

"Cisco has announced patches to address four critical security flaws impacting Identity Services and Webex Services that could result in arbitrary code execution and allow an attacker to impersonate any user within the service."

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

https://thehackernews.com/2026/04/cisco-patches-four-critical-identity.html

AVideo YPTSocket WebSocket Broadcast Relay Leads To Unauthenticated Cross-User JavaScript Execution Via Client-Side Eval() Sinks

"The YPTSocket plugin's WebSocket server relays attacker-supplied JSON message bodies to every connected client without sanitizing the msg or callback fields. On the client side, plugin/YPTSocket/script.js contains two eval() sinks fed directly by those relayed fields (json.msg.autoEvalCodeOnHTML at line 568 and json.callback at line 95). Because tokens are minted for anonymous visitors and never revalidated beyond decryption, an unauthenticated attacker can broadcast arbitrary JavaScript that executes in the origin of every currently-connected user (including administrators), resulting in universal account takeover, session theft, and privileged action execution."
CERTVU recommends all users and organizations to read this vulnerability and follow the mitigation steps to mitigate these vulnerabilities.

https://github.com/WWBN/AVideo/security/advisories/GHSA-gph2-j4c9-vhhr

SAP Patches Critical ABAP Vulnerability

"SAP on Tuesday announced the release of 20 new and updated security notes as part of its April 2026 security patch day. The most severe of the resolved flaws is CVE-2026-27681 (CVSS score of 9.9), a critical SQL injection bug in Business Planning and Consolidation and Business Warehouse that could lead to arbitrary code execution. “The vulnerable ABAP program allows a low-privileged user to upload a file with arbitrary SQL statements that will then be executed,” software security firm Onapsis explains."
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-abap-vulnerability/

Juniper Networks Patches Dozens Of Junos OS Vulnerabilities

"Juniper Networks this week released patches for nearly three dozen vulnerabilities, including Junos OS and Junos OS Evolved bugs that could lead to privilege

escalation, denial-of-service (DoS), and command execution. The most severe of the flaws is CVE-2026-33784 (CVSS score of 9.8), a default password in the Support Insights (JSI) Virtual Lightweight Collector (vLWC) that could be exploited remotely to take over a vulnerable device. “vLWC software images ship with an initial password for a high-privileged account. A change of this password is not enforced during the provisioning of the software, which can make full access to the system by unauthorized actors possible,” Juniper Networks explains."
CERTVU recommends all users and organizations to read this Vulnerability and follow the mitigation steps to mitigate these vulnerabilities.

https://www.securityweek.com/juniper-networks-patches-dozens-of-junos-os-vulnerabilities/

Flowise AI Agent Builder Under Active CVSS 10.0 RCE Exploitation; 12,000+ Instances Exposed

"Threat actors are exploiting a maximum-severity security flaw in Flowise, an open-source artificial intelligence (AI) platform, according to new findings from VulnCheck. The vulnerability in question is CVE-2025-59528 (CVSS score: 10.0), a code injection vulnerability that could result in remote code execution. "The CustomMCP node allows users to input configuration settings for connecting to an external MCP (Model Context Protocol) server," Flowise said in an advisory released in September 2025. "This node parses the user-provided mcpServerConfig string to build the MCP server configuration. However, during this process, it executes JavaScript code without any security validation."
CERTVU recommends all users and organizations to read this Vulnerability and follow the mitigation steps to mitigate these vulnerabilities.

https://thehackernews.com/2026/04/flowise-ai-agent-builder-under-active.html

50,000 WordPress Sites Affected By Arbitrary File Upload Vulnerability In Ninja Forms – File Upload WordPress Plugin

"On January 8th, 2026, we received a submission for an Arbitrary File Upload vulnerability in Ninja 1/8 Forms – File Upload, a WordPress plugin with an estimated 50,000 active installations. This vulnerability makes it possible for an unauthenticated attacker to upload arbitrary files to a vulnerable site and achieve remote code execution."
CERTVU recommends all users and organizations to read this Vulnerability and follow the mitigation steps to mitigate these vulnerabilities.

https://www.wordfence.com/blog/

2026/04/50000-wordpress-sites-affected-by-arbitrary-file-upload-vulnerability-in-ninjaforms-file-upload-wordpress-plugin/

Critical Cisco IMC Auth Bypass Gives Attackers Admin Access

"Cisco has released updates to address a critical security flaw in the Integrated Management Controller (IMC) that, if successfully exploited, could allow an unauthenticated, remote attacker to bypass authentication and gain access to the system with elevated privileges. The vulnerability, tracked as CVE-2026-20093, carries a CVSS score of 9.8 out of a maximum of 10.0. "This vulnerability is due to incorrect handling of password change requests," Cisco said in an advisory released Wednesday. "An attacker could exploit this vulnerability by sending a crafted HTTP request to an affected device."
CERTVU recommends all users and organizations to read this Vulnerability and follow the mitigation steps to mitigate these vulnerabilities.

https://thehackernews.com/2026/04/cisco-patches-98-cvss-imc-and-ssm-flaws.html `

Malware

MCPwn: A CVSS 9.8 One-Line MCP Bug That Hands Over Your Nginx To Anyone On The Network – Actively Exploited In The Wild

"What if a single missing function call – one middleware reference, 27 characters – could give any attacker on your network complete control over your nginx web server? No credentials needed. No exploitation complexity. Just a plain HTTP request to a URL that should have been protected but wasn't. That's CVE-2026-33032, a critical vulnerability (CVSS 9.8) we discovered in nginx-ui, a popular web based nginx management tool with over 11K GitHub stars and 430,000+ Docker pulls. Since publication, active exploitation in the wild has been confirmed: VulnCheck added it to their Known Exploited Vulnerabilities (KEV) list, and Recorded Future's Insikt Group identified it as one of 31 high impact CVEs actively exploited in March 2026, assigning it a Risk Score of 94/100 alongside vulnerabilities in Cisco, Microsoft, Google, and Citrix."

https://pluto.security/blog/mcp-bug-nginx-security-vulnerability-cvss-9-8/

Three Microsoft Defender Zero-Days Actively Exploited; Two Still Unpatched

"Huntress is warning that threat actors are exploiting three recently disclosed security flaws in Microsoft Defender to gain elevated privileges in compromised systems. The activity involves the exploitation of three vulnerabilities that are codenamed BlueHammer (requires GitHub sign-in), RedSun, and UnDefend, all of which were released as zero-days by a researcher known as Chaotic Eclipse (aka Nightmare-Eclipse) in response to Microsoft's handling of the vulnerability disclosure process. While both Blue Hammer and Red Sun are local privilege escalation (LPE) flaws impacting Microsoft Defender, UnDefend can be used to trigger a denial-of-service (DoS) condition and effectively block definition updates."

https://thehackernews.com/2026/04/three-microsoft-defender-zero-days.html

Axios Compromised On Npm - Malicious Versions Drop Remote Access Trojan

"Step Security is hosting a community town hall on this incident on April 1st at 10:00 AM PT - Register Here. axios is the most popular JavaScript HTTP client library with over 100 million weekly downloads. On March 30, 2026, StepSecurity identified two malicious versions of the widely used axios HTTP client library published to npm: axios@1.14.1 and axios@0.30.4. The malicious versions inject a new dependency, plain-crypto-js@4.2.1, which is never imported anywhere in the axios source code. Its sole purpose is to execute a postinstall script that acts as a cross platform remote access trojan (RAT) dropper, targeting macOS, Windows, and Linux. The dropper contacts a live command and control server and delivers platform specific second stage payloads. After execution, the malware deletes itself and replaces its own package. Json with a clean version to evade forensic detection."

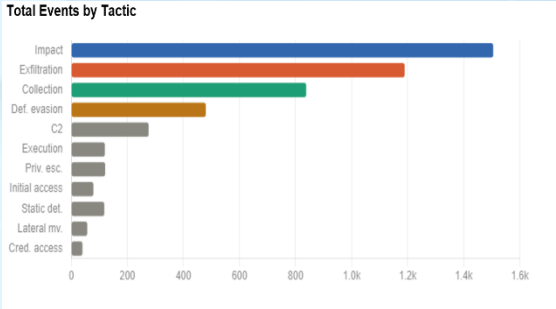
https://www.stepsecurity.io/blog/axios-compromised-on-npm-malicious-versions-drop-remote-access-trojan

CERTVU Threat Statistics

Attack index summary

This report provides an analysis of cyber-attack telemetry recorded by CERT Vanuatu during April 2026. A total of **4,823 events** were captured across 13 MITRE ATT&CK tactic categories over the 30-day reporting period.
The month was characterized by sustained high-impact and exfiltration activity, with a notable escalation in adversarial sophistication during the third week (April 15–21), where

credential access, lateral movement, and command-and-control tactics were detected in close succession — a pattern consistent with an active, multi-stage intrusion campaign.
Static detection capability was absent for the first 12 days, activating from April 13 onward. This represents a significant detection gap that should be addressed in the operational response plan.



Key metrics

4,823 Total events recorded	**1,505** Top tactic (Impact)	**1,189** Exfiltration events	**12** Detection gap (days)	**3** Near-silent days

Tactic-by-Tactic Breakdown

The table below presents total event counts for each MITRE ATT&CK tactic category recorded during April 2026, along with a proportional share and assessed risk level.

Tactic	Total events	Share of total
Impact	1,505	31%
Exfiltration	1,189	25%
Collection	838	17%
Defense evasion	480	10%
Command & control	276	6%
Execution	120	2%
Privilege escalation	121	3%
Initial access	79	2%
Static detection	118	2%
Lateral movement	57	1%
Credential access	40	1%
Persistence	0	0%
Discovery	0	0%

Note: Persistence and Discovery recorded zero events throughout the reporting p may indicate coverage gaps rather than genuine absence of adversarial activity i categories.

CERTVU Advisories

The Department of Communication and Digital Transformation (DCDT) through CERT Vanuatu (CERTVU), provides the following advisory.

Advisory 140: CISCO - FIRESTARTER Backdoor (CVE-2025-20333) & (CVE-2025-20362)

These advisories cover two critical vulnerabilities in Cisco's network security products — Adaptive Security Appliance (ASA) and Firepower Threat Defense (FTD) software — that have been actively exploited together by a sophisticated, state-sponsored Advanced Persistent Threat (APT) actor known as UAT-4356 (also tracked as ArcaneDoor and Storm-1849).
What makes this campaign exceptionally dangerous is a second stage: even after organisations patch the two CVEs, a custom-built backdoor called FIRESTARTER may already be embedded in the device. Patching alone does not remove it. The threat actor can continue to access the compromised device indefinitely unless specific additional steps are taken.

https://cert.gov.vu/index.php/advisories/149-advisory-141

Advisory 139: Microsoft Defender Insufficient Granularity of Access Control Vulnerability (CVE-2026-33825)

CVE-2026-33825 is a high-severity vulnerability (CVSS ~8.6) in VMware vCenter Server. The flaw is caused by improper input validation (CWE-20) within specific API endpoints exposed by vCenter.

https://cert.gov.vu/index.php/advisories/148-advisory-139

Advisory 138: Apache ActiveMQ Improper Input Validation Vulnerability (CVE-2026-34197)

CVE-2026-34197 is a high-severity remote code execution (RCE) vulnerability (CVSS ~8.8) affecting Apache Tomcat.
The flaw is caused by improper input validation in HTTP request processing, specifically when handling certain malformed requests that can lead to memory corruption or unsafe object handling inside the server's request pipeline.

https://cert.gov.vu/index.php/advisories/144-advisory-138

Advisory 137: Microsoft SharePoint Server Improper Input Validation Vulnerability (CVE-2026-32201)

Microsoft SharePoint Server contains an improper input validation vulnerability that allows an unauthorized attacker to perform spoofing over a network.

https://cert.gov.vu/index.php/advisories/143-advisory-137

Advisory 136: Microsoft Office Remote Code Execution (CVE-2009-0238)

CVE-2009-0238 is a critical remote code execution vulnerability (CVSS ~9.3) in Microsoft Windows Internet Printing service (MS08-067-related RPC component exposure). It is caused by a stack-based buffer overflow in the handling of RPC requests over SMB (Server Message Block).
The flaw allows an attacker to send a specially crafted network request that overflows memory buffers in the Windows RPC service, enabling arbitrary code execution at SYSTEM level.

https://cert.gov.vu/index.php/advisories/142-advisory-136

Advisory 135: Fortinet FortiClient EMS SQL Injection Vulnerability (CVE-2026-21643)

An improper neutralization of special elements used in an sql command ('sql injection') vulnerability in Fortinet FortiClientEMS 7.4.4 may allow an unauthenticated attacker to execute unauthorized code or commands via specifically crafted HTTP requests.

https://cert.gov.vu/index.php/advisories/141-advisory-135

Advisory 134: Adobe Acrobat Use-After-Free Vulnerability (CVE-2020-9715)

CVE-2020-9715 is a critical remote code execution (RCE) vulnerability in Adobe Acrobat Reader DC and Adobe Acrobat.
The flaw is a use-after-free memory corruption vulnerability (CWE-416) that occurs when the application improperly handles objects in memory while processing specially crafted PDF files. When freed memory is accessed again, attackers can manipulate it to execute arbitrary code.

https://cert.gov.vu/index.php/advisories/140-advisory-134

Advisory 133: Microsoft Windows Out-of-Bounds Read Vulnerability (CVE-2023-36424)

CVE-2023-36424 is a high-severity elevation of privilege (EoP) vulnerability (CVSS 7.8) in Microsoft Windows. It affects the Windows Common Log File System (CLFS) driver, a core kernel component responsible for handling transactional logging.

https://cert.gov.vu/index.php/advisories/147-advisory-1333

Advisory 132: Microsoft Exchange Server Deserialization of Untrusted Data Vulnerability (CVE-2023-21529)

CVE-2023-21529 is a high-severity remote code execution (RCE) vulnerability affecting Microsoft Exchange Server. The flaw is caused by deserialization of untrusted data (CWE-502), where the application improperly processes serialized objects.
When Exchange Server deserializes attacker-controlled data without proper validation, it can execute malicious payloads embedded in that data, leading to arbitrary code execution on the server.

https://cert.gov.vu/index.php/advisories/139-advisory-132

Advisory 131: Microsoft Windows Link Following Vulnerability (CVE-2025-60710)

CVE-2025-60710 is a high-severity privilege escalation vulnerability (CVSS 7.8) affecting Microsoft Windows systems. The flaw exists in the Host Process for Windows Tasks, due to improper link resolution before file access.

https://cert.gov.vu/index.php/advisories/138-advisory-131

Advisory 130: Fortinet FortiClient EMS Improper Access Control Vulnerability

CVE-2012-1854 is a critical remote code execution vulnerability in Microsoft Windows, specifically within the Microsoft XML Core Services (MSXML) component used by Internet Explorer and other applications.
The flaw is caused by improper handling of objects in memory (use-after-free / memory corruption) when processing specially crafted web content. This allows attackers to corrupt memory and execute arbitrary code.

https://cert.gov.vu/index.php/advisories/137-advisory-130

Advisory 129: Fortinet FortiClient EMS Improper Access Control Vulnerability

CVE-2026-35616 is a critical remote code execution (RCE) vulnerability (CVSS 9.8) affecting Fortinet FortiClient Endpoint Management Server (EMS). The flaw is caused by improper access control (CWE-284) in the application's API.

Due to insufficient authentication enforcement, the system fails to properly restrict access to sensitive API endpoints. This allows attackers to send crafted requests that bypass authentication and execute unauthorized commands.
https://cert.gov.vu/index.php/advisories/136-advisory-129

Advisory 128: TrueConf Client Download of Code Without Integrity Check Vulnerability

CVE-2026-3502 is a high-severity vulnerability (CVSS ~8.1) affecting Atlassian Confluence deployments. The issue stems from improper input validation.
TrueConf Client contains a download of code without integrity check vulnerability. An attacker who is able to influence the update delivery path can substitute a tampered update payload. If the payload is executed or installed by the updater, this may result in arbitrary code execution in the context of the updating process or user.

https://cert.gov.vu/index.php/advisories/135-advisory-128

Upcoming Events

Cyber month Event

October is recognized as Cyber Month, a national initiative dedicated to promoting cybersecurity awareness and strengthening digital resilience across the country. As part of the Cyber Up Pacific campaign, CERT Vanuatu (CERTVU) leads a series of Cyber Week activities designed to educate and engage communities, schools, government agencies, and private sector organizations. Through awareness sessions, outreach programs, and capacity-building initiatives, CERTVU aims to foster a safer and more secure digital environment for all citizens.

CERT Vanuatu Efforts

CERT Vanuatu (CERT-VU) continues to play a key role in enhancing the nation's cybersecurity posture. Through close collaboration with government agencies, private sector organizations, international partners, and local communities, CERT-VU actively addresses emerging cyber threats and challenges. Its ongoing efforts in incident response, awareness, and capacity building contribute to creating a digitally informed society that is better equipped to prevent, respond to, and recover from cyber incidents.

Cybersecurity Awareness Program

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

Economic Micro Business Hub opening

The Department of Communication and Digital transformation (DCDT) through the Computer Emergency Response Team (CERTVU) has made cyber security awareness during the opening of the Economic Micro Business Hub at Emua village on the 8th of April 2026.

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

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

The roadmap will guide the adoption of cloud services across governments to improve efficiency and service delivery, while the Cybersecurity Agency will strengthen national cyber defenses through coordinated policy, oversight, and protection of digital assets.

Together, these initiatives support Vanuatu's goal of building a more secure and modern digital government.

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://thehackernews.com/2026/04/cisco-patches-98-cvss-imc-and-ssm-flaws.html
2. https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-cimc-auth-bypass-AgG2BxTn
3. https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ssm-cli-execution-cHUcWuNr
4. https://www.bleepingcomputer.com/news/security/critical-cisco-imc-auth-bypass-gives-attackers-admin-access/
5. https://securityaffairs.com/190295/security/cisco-fixed-critical-and-high-severity-flaws.html
7. https://www.securityweek.com/cisco-patches-critical-and-high-severity-vulnerabilities/
8. https://www.wordfence.com/blog/2026/04/50000-wordpress-sites-affected-by-arbitrary-file-upload-vulnerability-in-ninjaforms-file-upload-wordpress-plugin/
9. https://www.bleepingcomputer.com/news/security/hackers-exploit-critical-flaw-in-ninja-forms-wordpress-plugin/
10. https://thehackernews.com/2026/04/flowise-ai-agent-builder-under-active.html
11. https://github.com/FlowiseAI/Flowise/security/advisories/GHSA-3gcm-f6qx-ff7p
12. https://www.bleepingcomputer.com/news/security/max-severity-flowise-rce-vulnerability-now-exploited-in-attacks/
13. https://www.securityweek.com/critical-flowise-vulnerability-in-attacker-crosshairs/
14. https://securityaffairs.com/190471/security/attackers-exploit-critical-flowise-flaw-cve-2025-59528-for-remote-codeexecution.html
15. https://www.securityweek.com/juniper-networks-patches-dozens-of-junos-os-vulnerabilities/
16. https://www.securityweek.com/sap-patches-critical-abap-vulnerability/
17. https://thehackernews.com/2026/04/cisco-patches-four-critical-identity.html
18. https://www.securityweek.com/cisco-patches-critical-vulnerabilities-in-webex-ise/
19. https://www.bleepingcomputer.com/news/security/cisco-says-critical-webex-services-flaw-requires-customer-action/
20. https://securityaffairs.com/190909/security/cisco-fixed-four-critical-flaws-in-identity-services-and-webex.html
21. https://github.com/WWBN/AVideo/security/advisories/GHSA-gph2-j4c9-vhhr
22. https://kb.cert.org/vuls/id/915947
23. https://thehackernews.com/2026/04/sglang-cve-2026-5760-cvss-98-enables.html
24. https://www.wordfence.com/threat-intel/vulnerabilities/wordpress-plugins/breeze/breeze-cache-244-unauthenticatedarbitrary-file-upload-via-fetch-gravatar-from-remote
25. https://www.bleepingcomputer.com/news/security/hackers-exploit-file-upload-bug-in-breeze-cache-wordpress-plugin/

26. https://www.securityweek.com/vulnerabilities-patched-in-crowdstrike-tenable-products/
27. https://www.crowdstrike.com/en-us/security-advisories/cve-2026-40050/
28. https://securityaffairs.com/191343/hacking/critical-bug-in-crowdstrike-logscale-let-attackers-access-files.html
29. https://pluto.security/blog/mcp-bug-nginx-security-vulnerability-cvss-9-8/
30. https://thehackernews.com/2026/04/critical-nginx-ui-vulnerability-cve.html
31. https://www.bleepingcomputer.com/news/security/critical-nginx-ui-auth-bypass-flaw-now-actively-exploited-in-the-wild/
32. https://www.darkreading.com/application-security/critical-mcp-integration-flaw-nginx-risk
33. https://www.infosecurity-magazine.com/news/nginx-ui-mcp-flaw-actively/
34. https://www.securityweek.com/exploited-vulnerability-exposes-nginx-servers-to-hacking/
35. https://securityaffairs.com/190841/hacking/cve-2026-33032-severe-nginx-ui-bug-grants-unauthenticated-serveraccess.html
36. https://thehackernews.com/2026/04/three-microsoft-defender-zero-days.html
37. https://www.bleepingcomputer.com/news/security/recently-leaked-windows-zero-days-now-exploited-in-attacks/
38. https://www.helpnetsecurity.com/2026/04/17/microsoft-defender-zero-days-exploited/
39. https://securityaffairs.com/190961/hacking/microsoft-defender-under-attack-as-three-zero-days-two-of-them-still-unpatchedenable-elevated-access.html
40. https://www.facebook.com/CERTVU
41. https://cert.gov.vu/index.php/advisories