[TLP: CLEAR]

Monthly Security Bulletin– July 2026

Overview

Greetings,
CERT Vanuatu (CERTVU), under the Department of Communication and Digital Transformation (DCDT), is pleased to present its **July 2026 Security Bulletin**. This edition highlights key vulnerabilities and active cyber threats identified during the month across commonly used systems and applications. The bulletin is intended to help organizations improve their **cybersecurity awareness, preparedness, and resilience** against emerging threats.

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

Enterprise Tech In, Shell Out (Progress Kemp LoadMaster Uninitialized Heap To Pre-Auth RCE CVE-2026-8037)

"Welcome back to another watchTowr Labs blog post. This time, we're looking at Progress Kemp LoadMaster, a load balancer that sits at the edge of a lot of enterprise networks. Edge appliances have a habit of becoming the way in rather than the thing keeping people out, and CVE-2026-8037 keeps that streak alive: a pre-authentication Remote Code Execution vulnerability accessible to anyone who can access the API. So, in probably a predictable turn of events, we're back doing what we do best."
CERTVU recommends all users and organizations to read this vulnerability and follow the mitigation steps to mitigate these vulnerabilities.

https://labs.watchtowr.com/enterprise-tech-in-shell-out-progress-kemp-loadmaster-uninitialized-

heap-to-pre-auth-rce-cve2026-8037/

Adobe Security Bulletin

"Adobe has released security updates for ColdFusion versions 2025 and 2023.These updates resolves critical and important vulnerabilitiesthat could lead toarbitrary code execution, privilege escalation, arbitrary file system read, and security feature bypass. Adobe is not aware of any exploits in the wild for any of the issues addressed in these updates.
CERTVU recommends all users and organizations to read this vulnerability and follow the mitigation steps to mitigate these vulnerabilities.

https://helpx.adobe.com/security/products/coldfusion/apsb26-68.html

DuneSlide: Two Critical RCE Vulnerabilities Via Zero-Click Prompt Injection In Cursor IDE

"Cato AI Labs has discovered two critical remote code execution (RCE) vulnerabilities in Cursor IDE, the popular development environment which, according to Cursor, is used by over half of the Fortune 500. Both RCE vulnerabilities, which we refer to as "DuneSlide," achieved a 9.8 CVSS score, and involve breaking out of the IDE's sandbox environment and were assigned CVE IDs CVE-2026-50548 and CVE 2026-50549. Together, these vulnerabilities show how prompt injection can reach beyond the LLM layer and expose classical vulnerabilities in code paths that were not traditionally considered part of the attack surface."
CERTVU recommends all users and organizations to read this advisory and follow the mitigation steps to mitigate these vulnerabilities.

https://www.catonetworks.com/blog/duneslide-two-critical-rce-vulnerabilities/

Security Advisory Bulletin 066

"A malicious actor with access to the network could exploit an Improper Access Control vulnerability found in UniFi Connect Application to execute a Command Injection on the host device."
CERTVU recommends all users and organizations to read this advisory and follow the mitigation steps to mitigate these vulnerabilities.

https://community.ui.com/releases/Security-Advisory-Bulletin-066-066/984eceb3-49c8-4227-942d-671c289b3afc

SonicWall Warns Of SMA1000 Flaws Exploited In Zero-Day Attacks, Patch Now

"SonicWall warns that threat actors have been exploiting two SMA1000 vulnerabilities, tracked as

CVE 2026-15409 and CVE-2026-15410, in zero-day attacks and urges customers to install the newly released security updates. CVE-2026-15409 is a critical (CVSS 10.0) server-side request forgery (SSRF) vulnerability in the SMA1000 Appliance Work Place interface that allows a remote, unauthenticated attacker to force an appliance to make requests to unintended locations. CVE-2026-15410 is a high severity (CVSS 7.2) post-authentication code injection flaw in the SMA1000 Appliance Management Console that could allow a remote authenticated administrator to execute arbitrary operating system commands."
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/sonicwall-warns-of-sma1000-flaws-xploited-in-zero-day-attacks-patchnow/

SAP Warns Of Critical Flaws In NetWeaver And Commerce Cloud

"SAP has addressed 16 vulnerabilities across multiple products as part of its July 2026 security updates, including three critical flaws in NetWeaver, Commerce Cloud, and AppRouter. The first critical issue patched this month is a memory corruption security issue (tracked as CVE-2026-44747) stemming from an out-of-bounds write weakness in the NetWeaver Application Server ABAP (AS ABAP), the runtime environment, application server, and development platform for core SAP enterprise software."
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/sap-warns-of-critical-flaws-in-netweaver-and-commerce-cloud/

7 Severe Vulnerabilities Patched In VMware Avi Load Balancer

"Broadcom announced on Tuesday that new VMware Avi Load Balancer updates patch several critical and high-severity vulnerabilities. VMware Avi Load Balancer is a software-defined platform that provides load balancing, application security, and analytics for applications in hybrid and multi-cloud environments. According to Broadcom, two external researchers recently discovered that the VMware product is affected by seven potentially serious vulnerabilities."
CERTVU recommends all users and organizations to read this Vulnerability and follow the mitigation steps to mitigate these vulnerabilities.

https://www.securityweek.com/7-severe-vulnerabilities-patched-in-vmware-avi-load-balancer/

Zoom Warns Of Critical Account Takeover Vulnerability

"Zoom is warning of a critical vulnerability in its desktop client and software development kit for Windows that could be exploited by an unauthenticated party to hijack accounts. Discovered internally, the security issue is tracked as CVE-2026-53412 and received a severity score of 9.8 out of 10. In an advisory this week, the messaging platform says that the flaw affects Zoom Workplace for Windows before version 7.0.0, the Windows VDI Client before versions 7.0.10, 6.6.15, and 6.5.18, and the Meeting SDK for Windows before version 7.0.0."
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/zoom-warns-of-critical-account-takeover-vulnerability/

Vulnerabilities Patched By Fortinet, Ivanti, ServiceNow

"Fortinet, Ivanti, and ServiceNow on Tuesday rolled out patches for 15 vulnerabilities across their products. ServiceNow resolved a critical remote code execution (RCE) flaw in the ServiceNow AI platform that can be exploited without authentication. The bug is tracked as CVE-2026-6875 (CVSS score of 9.5). “ServiceNow addressed this vulnerability by deploying a security update to hosted instances. Relevant security updates have also been provided to ServiceNow self-hosted customers and partners,” the company said. Ivanti released fixes for two security defects in its data aggregation and visualization tool Xtraction, tracked as CVE-2026-14902 and CVE-2026-14903."
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-by-fortinet-ivanti-servicenow/

Oracle Patches Over 1,400 Vulnerabilities With Quarterly Security Updates

"Oracle has patched more than 1,400 vulnerabilities with its July 2026 Critical Patch Update (CPU), with a vast majority of the flaws likely identified by artificial intelligence. According to Oracle, the latest quarterly CPU includes 1,449 security patches, addressing 1,434 unique CVEs across 334 products. Vulnerabilities have been patched in products such as Database Server, APEX,

Autonomous Health Framework, Essbase, Global Lifecycle Management, GoldenGate, NoSQL Database, Spatial Studio, SQL Developer, TimesTen In-Memory Database, Application Testing Suite, Commerce, Communications, Construction and Engineering, and E-Business Suite."
CERTVU recommends all users and organizations to read this Vulnerability and follow the mitigation steps to mitigate these vulnerabilities.

https://www.securityweek.com/oracle-patches-over-1400-vulnerabilities-with-quarterly-security-updates/

2/8 Arista Patches VeloCloud Orchestrator Zero-Day Exploited In Attacks

"Arista has patched a maximum-severity command injection vulnerability in on-premises VeloCloud Orchestrator deployments that is being actively exploited in attacks. The vulnerability, tracked as CVE 2026-16812, is an unauthenticated OS command injection flaw with severity scores of 10.0, the maximum score that can be given to flaws. VeloCloud Orchestrator, also known as VCO, is a centralized management platform used to configure, monitor, and manage VeloCloud SD-WAN deployments and associated edge devices."

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/arista-patches-velocloud-orchestrator-zero-day-exploited-in-attacks/

RufRoot: The MCP Bridge Vulnerability That Turns Agents Into Rogue Admins (CVE-2026-59726)

"Noma Labs found a critical (10 CVSS) vulnerability in Ruflo, an open source AI agent orchestration platform with more than 67,000 GitHub stars at the time of this writing and ranked #2 on MCPMarket. Ruflo ships with a chat UI, agent swarms, persistent memory, and MCP-based tool calling. The platform's MCP Bridge, the Express.js server that handles all tool invocations, exposes 233 tools over HTTP with zero authentication. Noma Labs researchers got one of those tools to run arbitrary shell commands. A single unauthenticated HTTP POST request to port 3001 gave full command execution inside the container. No token, no API key, no header check, no IP allowlist. Nothing."
CERTVU recommends all users and organizations to read this Vulnerability and follow the mitigation steps to mitigate these vulnerabilities.

https://noma.security/blog/rufroot-the-mcp-bridge-vulnerability-that-turns-agents-into-rogue-admins-cve-2026-59726/

Three Critical VMware Flaws Allow Auth Bypass, Code Execution, And VM Escape

"Broadcom has released security updates to address multiple security flaws impacting VMware ESX, vCenter, Workstation, and Fusion, three of which have been designated as critical in severity. The first of the three critical-rated flaws is CVE-2026-59309 (CVSS score: 9.8), which has been described as an authentication bypass in VMware vCenter. "A malicious actor with network access to vCenter may exploit this issue to bypass authentication and gain unauthorized access to the system," Broadcom said."
CERTVU recommends all users and organizations to read this Vulnerability and follow the mitigation steps to mitigate these vulnerabilities.

https://thehackernews.com/2026/07/three-critical-vmware-flaws-allow-auth.html

Critical Rails Flaw Could Let Unauthenticated Attackers Read Server Files Via Image Uploads

"Ruby on Rails has released fixes for a critical Active Storage vulnerability that could let unauthenticated attackers read arbitrary files from application servers through crafted image uploads. Tracked as CVE-2026-66066 (CVSS score: 9.5), the flaw can expose the Rails process environment and secrets such as secret_key_base, the Rails master key, database passwords, cloud storage credentials, and API tokens. Those secrets may enable remote code execution (RCE) or lateral movement into connected systems. Affected applications use libvips for Active Storage image processing and accept image uploads from untrusted users. Rails selects Vips under load_defaults 7.0, and later defaults retain it."
CERTVU recommends all users and organizations to read this Vulnerability and follow the mitigation steps to mitigate these vulnerabilities.

https://thehackernews.com/2026/07/critical-rails-flaw-could-let.html

New Gitea RCE Lets Repository Writers Plant a Git Hook To Run Shell Commands

"Gitea, the self-hosted Git platform, has patched a critical remote code execution vulnerability. A user with ordinary repository write access can turn attacker-controlled patch content into a live Git hook and run shell commands as the Gitea service account. Tracked as CVE-2026-60004 (CVSS score: 9.8), the

flaw affects Gitea versions 1.17 and later before 1.27.1 and is fixed in 1.27.1. The vulnerable API call requires authentication and repository write permission. But Gitea enables registration by default, so an outside visitor can create a normal account and repository on an unchanged installation, then exploit the bug without pre-existing credentials."
CERTVU recommends all users and organizations to read this Vulnerability and follow the mitigation steps to mitigate these vulnerabilities.

https://thehackernews.com/2026/07/new-gitea-rce-lets-repository-writers.html

Malware

Exploitation In The Wild Of Wp2shell

"Wiz Research has identified exploitation of "wp2shell", a critical pre-auth RCE vulnerability chain impacting WordPress Core (CVE-2026-63030 & CVE-2026-60137). Attackers are deploying persistent webshells on vulnerable servers. Organizations should prioritize patching or applying WAF mitigations."

https://www.wiz.io/blog/wp2shell-cve-2026-63030-cve-2026-60137

Critical ServiceNow Code Execution Flaw Now Exploited In Attacks

"Attackers have begun exploiting a critical vulnerability (CVE-2026-6875) in the ServiceNow AI Platform, according to threat intelligence company Defused. Formerly known as the Now Platform, ServiceNow AI Platform is an enterprise-grade Platform-as-a-Service (PaaS) that helps businesses integrate AI into core enterprise workflows. Cybersecurity company Searchlight Cyber, which found this critical vulnerability and reported it on April 1st, says that it allows unauthenticated threat actors to escape the sandbox and execute code remotely within the ServiceNow platform in high-complexity attacks."

https://www.bleepingcomputer.com/news/security/critical-servicenow-code-execution-flaw-now-exploited-in-attacks/

Max Severity Adobe ColdFusion Flaw Now Exploited In Attacks

"Attackers are now exploiting a maximum-severity Adobe ColdFusion vulnerability tracked as CVE-2026 48282, according to vulnerability intelligence company KEVIntel. ColdFusion is a commercial web app development platform designed to help build and deploy enterprise-grade websites. The CVE-2026 48282 security flaw

affects ColdFusion versions 2025.9, 2023.20, and earlier, and can be exploited by attackers without privileges to gain remote code execution on unpatched systems. Adobe released security updates on Tuesday to address the vulnerability, saying that it posed a high risk of exploitation and urging admins to deploy patches immediately."

https://www.bleepingcomputer.com/news/security/max-severity-adobe-coldfusion-flaw-now-exploited-in-attacks/

Threat Actors Probe Gitea Docker Flaw CVE-2026-20896 13 Days After Disclosure

"Threat actors have been observed attempting to exploit a recently patched critical security flaw in Gitea Docker images, according to Sysdig. The vulnerability in question is CVE-2026-20896 (CVSS score: 9.8), a vulnerability that stems from the DevOps platform trusting the "X-WEBAUTH-USER" header from any source IP address, effectively allowing an unauthenticated internet client to get elevated access."

https://thehackernews.com/2026/07/threat-actors-probe-gitea-docker-flaw.html>

New Dysphoria DDoS Botnet Spreads To 200k Devices Worldwide

"A botnet called Dysphoria has compromised around 200,000 devices across the world and is using them for distributed denial of service (DDoS) attacks and traffic relay operations. According to QiAnXin XLab cybersecurity researchers, Dysphoria evolved from the 'jackskid' and 'fbot' malware by adding a covert blockchain-based command-and-control (C2) resolution mechanism. Specifically, the botnet uses Ethereum ENS and Solana SNS domains to retrieve infrastructure information, while C2 addresses are concealed inside fake IPv6 strings and recovered using a custom byte-transformation algorithm."

https://www.bleepingcomputer.com/news/security/new-dysphoria-ddos-botnet-spreads-to-200k-devices-worldwide/

MedusaHVNC: A Hidden Desktop That Steals Live Windows Sessions

"We recently came across a sample of MedusaHVNC, a new remote access trojan (RAT) being sold as malware-as-a-service (MaaS). When we took it apart, we found a hidden virtual network computing (HVNC) module that opens a browser on a separate Windows desktop, out of sight of the victim. The browser still runs on the victim's device, so it can load an existing profile, including cookies and session state. This gives the

operator access to live, logged-in sessions while the activity continues to come from the victim's usual machine."

https://www.blackfog.com/medusahvnc-a-hidden-desktop/

Helpdesk Hijackers: Teams Vishing, Quick Assist, And GoGRPC Backdoor

"Zscaler ThreatLabz has been tracking attacks from a threat actor that is likely an initial access broker for ransomware attacks since January 2026. The threat actor targets organizations by leveraging vishing techniques through Microsoft Teams and deploying a variety of tools including a Go-based backdoor that we named GoGRPC. ThreatLabz has identified at least four variants of GoGPRC that we named Lep, Giver, Pet, and Kind. In some instances, the threat actor has deployed additional malware tools that include a backdoor that we named BlindDoor, a Go-based reverse SOCKS proxy we named RevSocket, a Python-based reverse SOCKS proxy we named PyGRPC, and two other tools we named S3Siphon and RSOX."

https://www.zscaler.com/blogs/security-research/helpdesk-hijackers-teams-vishing-quick-assist-and-gogrpc-backdoor

Operation BlueDash: Multi-RMM Workplace Phishing

"ZeroBEC investigated a live Microsoft Teams-themed phishing operation that began with a "secure document" email and ended with the silent enrollment of the victim endpoint into attacker-controlled remote monitoring and management environments. The victim was directed through compromised web infrastructure to a counterfeit Microsoft Store page claiming that Microsoft Teams had to be updated before the shared document could be opened. The active download delivered supportdev.exe, an Inno Setup-based loader that launched PowerShell in a hidden window, retrieved the official Level RMM installer, and registered the endpoint using an attacker-controlled enrollment secret. The same command attempted to deploy ScreenConnect in parallel, providing a redundant remote-access channel."

https://zerobec.com/blog/operation-bluedash-multi-rmm-workplace-phishing

Check And Protect: Analysis Of Telegram Phishing Operation Targeting Exiled Activist

"In July 2026, RESIDENT.NGO investigated an instance of a cloaked Telegram phishing campaign used against an exiled

Belarusian activist living in Lithuania. Delivered in a private Telegram Secret Chat as a fake Telegram security alert, the phishing link led to a convincing Telegram-themed page designed to capture one-time login codes in real time. The operation's defining feature was not the phishing page itself but its browser- and device-aware cloaking: visitors using browser and platform configurations accepted by the server, together with a syntactically valid token, could receive the phishing interface, while other configurations—including many automated scanners and some common desktop browsers— were shown decoy content or redirected to Telegram's legitimate website."

https://resident.ngo/lab/writeups/check-and-protect-analysis-of-telegram-phishing-operation-targeting-exiled-activist/

DinDoor, DenoRAT, And NightshadeC2: Analyzing TAG-150's Evolving Tradecraft

"In June 2026, eSentire's Threat Response Unit (TRU) disrupted a malicious ClickFix-style command in a Finance customer's environment. Further investigation found that the command installs DinDoor, a Deno-based loader, DenoRAT, a Deno-based Remote Access Trojan (RAT), and NightshadeC2, a sophisticated RAT and information stealer associated with TAG-150, a threat group active since March 2025."

https://www.esentire.com/blog/dindoor-denorat-and-nightshadec2-analyzing-tag-150s-evolving-tradecraft

APT42: AI-Assisted Rapport Phishing And a More Resilient TAMECAT

"APT42 continues to refine a familiar operating model, making it harder to detect and easier to scale. Three developments define the current picture. SpearSpecter combined prolonged WhatsApp engagement, Windows search-ms and WebDAV abuse, and a substantially expanded TAMECAT backdoor. APT42 also incorporated generative AI into target research, persona and pretext development, translation, malware engineering, debugging, code generation, and exploitation research. In March 2026, TA453 activity overlapping APT42 targeted a US think tank with a live credential phishing operation during an active regional conflict."

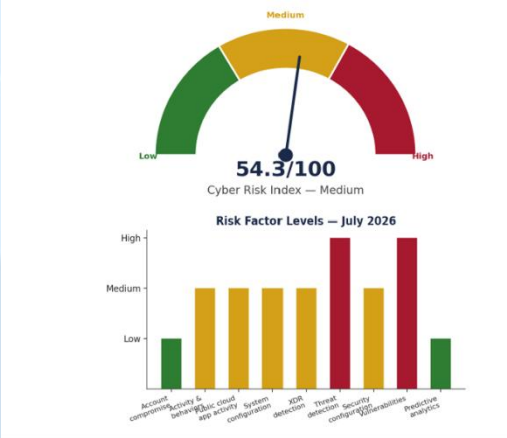
https://darkatlas.io/blog/apt42-ai-assisted-phishing-tamecat-analysis

CERTVU Threat Statistics

This bulletin summarises CERTVU's full Monthly Cybersecurity Report for July 2026 (reporting period 1–31 July, generated 3 August 2026). It draws on TrendAI Vision One

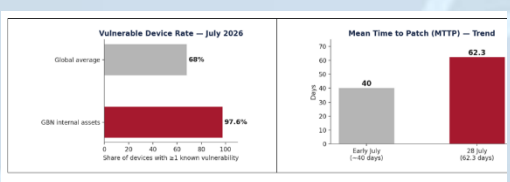
telemetry covering the Government Broadband Network — one infrastructure component within CERTVU's national CERT remit — together with partner data from CERT-Bund/BSI, CISA, KrCERT/CC and Shadowserver. Full technical detail sits in the source report and referenced advisories.

Overall risk Posture



Vulnerability management

Vulnerability management remains CERTVU's principal area of concern this month. Internal asset CVE density ran at roughly 7 to 10 times the global average, and Mean Time to Patch moved in the wrong direction — rising from around 40 days early in July to a monthly high of 62.3 days by 28 July.



The largest unpatched backlogs sit on ME-VM-iGOVDB01.vangov.local and ME-VM-CUSTOMSFS.vangov.local — each carrying 2,000 highly-exploitable CVEs at over 1,290 days unpatched, on end-of-support Windows Server 2012 R2 / 2019 builds. Both are flagged for priority remediation or decommissioning.

Major incident Spotlight

Multi-stage intrusion via Joomla compromise and Kerberos AS-REP Roasting (1 July)

On 1 July, attackers compromised a public-facing Joomla hosting environment and used reused credentials to pivot into the cloud control plane and, via CVE-2022-33679 (Kerberos AS-REP Roasting) against domain controller ME-VM-DC07, into Active Directory. They cracked a domain user account and moved laterally across four domain controllers using 27+ SMB connections, including a 28-second synchronised multi-DC window consistent with automated tooling. Impact included web defacement, unauthorised cryptomining, cloud control-plane compromise, and disruption to AD-dependent authentication. The source endpoint was isolated and the incident contained; full scope of exfiltration and persistence remained under investigation at report date. Two correlated incidents at maximum severity

(100/100) remained open at month end. Full detail: CERTVU Incident Report — Kerberos CVE-2022-33679 AS-REP Roasting Attack (1 July 2026).

Regional watch

July was an unusually active month for developments capable of fuelling misinformation or impersonation campaigns: criticism of the Nakamal Agreement from the Malvatumauri National Council of Chiefs, breakdown of sovereignty talks with France over Matthew and Hunter Islands (leading to a Special Envoy appointment on 30 July), and a contested Melanesian Spearhead Group Director-General appointment. CERTVU is factoring this heightened political sentiment into monitoring priorities alongside the technical threat landscape, alongside DCDT's public awareness advisory on harmful digital communications.

CERTVU Advisories

Advisory 182: BADBOX 2.0 Botnet Infections Detected on Consumer Internet-Connected Devices in Vanuatu

A botnet built from compromised Internet of Things (IoT) and Android-based consumer devices, used to provide criminal residential proxy services.
BADBOX 2.0 infects devices in two ways: some are shipped with backdoor malware already installed before purchase, and others are infected during set-up when the user is prompted to install applications from unofficial marketplaces. Once connected to a home or office network, the device joins the botnet and is enrolled into residential proxy services that allow criminals to route their traffic through the victim's internet connection.
The botnet succeeded the original BADBOX campaign, identified in 2023 and disrupted in 2024, and is assessed to consist of millions of devices worldwide. It has been the subject of international alerts and law enforcement action since 2023, summarised below.
CERTVU notes that no new international alert on BADBOX 2.0 has been issued since the FBI Public Service Announcement, which remains the current standing warning. Despite the threat having been publicly known for more than a year, infected devices remain active in Vanuatu.

https://cert.gov.vu/index.php/advisories/195-advisory-182

Advisory 178: Advisory 178: Adobe Campaign Classic Critical Vulnerability – Arbitrary Code Execution (CVE-2026-48449, CVSS 10.0)

Adobe has released security updates addressing two vulnerabilities in Adobe Campaign

Classic (ACC), its enterprise marketing automation platform. The most severe, CVE-2026-48449 (CWE-863, Incorrect Authorization), carries the maximum CVSS v3.1 base score of 10.0 and could result in arbitrary code execution in the context of the current user without requiring any user interaction. A second flaw, CVE-2026-48448 (CWE-89, SQL Injection), scores 8.6 and could allow arbitrary file system read. Adobe states it is not aware of either vulnerability being exploited in the wild. Separately, Adobe has also released updates for Adobe Bridge addressing eight Critical-rated vulnerabilities that could lead to privilege escalation and arbitrary code execution.

https://cert.gov.vu/index.php/advisories/190-advisory-178

Advisory 177: Google Chrome Multiple Vulnerabilities – Stable Channel Update (Chrome 151, 370 Fixes Including 7 Critical)

Google has released Chrome 151 to the Stable channel, fixing 370 security vulnerabilities, including 7 rated Critical, most of which are memory-safety issues (use-after-free, race conditions, and insufficient input validation) in core browser components. This follows Chrome 149 and 150, which together fixed 1,072 flaws, more than the prior 23 milestones combined, a surge Google and researchers attribute in part to AI-assisted vulnerability discovery.

https://cert.gov.vu/index.php/advisories/189-advisory-177

Advisory 176: Cisco Secure Firewall Management Center (FMC) Static Credential Vulnerability (CVE-2026-20316)

CVE-2026-20316 is a vulnerability in Cisco Secure Firewall Management Center (FMC) Software (CWE-259, Use of Hard-coded Password; CVSS v3.1 base score 5.3, Medium) caused by the presence of static user credentials for a low-privileged account in the FMC web-based management interface. Although the CVSS base score is Medium, Cisco has assigned this vulnerability a Security Impact Rating (SIR) of High, because the low-privileged access it grants can be combined with other Cisco Secure Firewall Management Center vulnerabilities to elevate privileges. Cisco has confirmed active exploitation of this vulnerability in the wild.

https://cert.gov.vu/index.php/advisories/188-advisory-176

Advisory 175: Arista VeloCloud Orchestrator (VCO) On-Prem OS Command Injection Vulnerability (CVE-2026-16812)

CVE-2026-16812 is a critical OS command injection vulnerability (CWE-78, CVSS v3.1 10.0) affecting

the on-premises deployment of Arista VeloCloud Orchestrator (VCO) - the SD-WAN management/orchestration platform for VeloCloud Edge devices (formerly VeloCloud by Broadcom).

https://cert.gov.vu/index.php/advisories/186-advisory-175

Advisory 174: Fortinet FortiOS SSL-VPN Symlink Persistence Patch Bypass (CVE-2025-68686)

Fortinet FortiOS SSL-VPN contains an Exposure of Sensitive Information to an Unauthorized Actor vulnerability (CWE-200), officially titled "SSL-VPN Symlink Persistence Patch Bypass" (FortiGuard advisory FG-IR-25-934), which may allow a remote, unauthenticated attacker to bypass the patch Fortinet previously developed for a symbolic-link persistence mechanism observed in earlier post-exploitation cases, via crafted HTTP requests.
Devices that never had SSL-VPN enabled are not affected by this issue.

https://cert.gov.vu/index.php/advisories/185-advisory-174

Advisory 173: Microsoft SharePoint Server Deserialization of Untrusted Data Vulnerability (CVE-2026-50522)

Microsoft SharePoint Server contains a deserialization of untrusted data vulnerability (CWE-502) that allows an unauthenticated attacker to execute arbitrary code over a network, with no user interaction required. The vulnerability carries a CVSS v3.1 base score of 9.8 (Critical), and Microsoft has assessed it as "Exploitation More Likely."
A working exploit for this vulnerability was first demonstrated at Pwn2Own Berlin and provided to Microsoft ahead of a fix. Despite this responsible disclosure, active in-the-wild exploitation only began after a public proof-of-concept was released on 20 July 2026, with successful attacks against internet-facing, unpatched on-premises SharePoint servers observed within hours. CVE-2026-50522 is the fourth SharePoint Server vulnerability confirmed under active exploitation in the current wave, alongside CVE-2026-32201 (addressed in CERTVU Advisory 137), CVE-2026-45659, CVE-2026-56164 and CVE-2026-58644.

https://cert.gov.vu/index.php/advisories/184-advisory-173

Advisory 172: WordPress Core SQL Injection Vulnerability_CVE-2026-60137

CVE-2026-60137 is a SQL injection vulnerability in the author__not_in

parameter of WP_Query, the core WordPress class responsible for building most of the database queries WordPress issues. It is classified as CWE-89 and carries a CVSS v3.1 base score of 9.1 (Critical) on its own.
This vulnerability is the companion flaw referenced in CERTVU Advisory 171 (CVE-2026-63030, the "wp2shell" REST API batch-route confusion issue). On WordPress 6.9 and higher, this SQL injection combines with CVE-2026-63030 to reach full unauthenticated remote code execution, publicly tracked as the "wp2shell" attack chain. On the 6.8.x branch, WordPress states this SQL injection is independently exploitable even though that branch is not listed as vulnerable to the full RCE chain.

https://cert.gov.vu/index.php/advisories/183-advisory-172

Advisory 171: WordPress Core REST API Batch-Route Confusion ("wp2shell") Vulnerability

CVE-2026-63030 is a REST API batch-route confusion vulnerability in WordPress Core, publicly referred to as "wp2shell," that allows an unauthenticated attacker to reach code paths that should require authentication.
On its own, the weakness is bounded. Its severity comes from its ability to unlock a second, more serious flaw - CVE-2026-60137.

https://cert.gov.vu/index.php/advisories/182-advisory-171

Advisory 170: Microsoft SharePoint Deserialization of Untrusted Data Vulnerability

CVE-2026-58644 is a remote code execution flaw caused by the deserialization of untrusted data that allows an unauthenticated threat actor to execute code remotely on a vulnerable SharePoint Server.
The vulnerability is a critical RCE vulnerability affecting Microsoft SharePoint Server with a CVSS score of 9.8. It stems from a deserialization of untrusted data flaw (CWE-502) and is remotely exploitable with low attack complexity.

https://cert.gov.vu/index.php/advisories/181-advisory-170

Advisory 169: Fortinet FortiSandbox OS Command Injection Vulnerability

CVE-2026-39808 is an improper neutralization of special elements used in an OS command (OS command injection) vulnerability in Fortinet FortiSandbox 4.4.0 through 4.4.8 that may allow an attacker to execute unauthorized code or commands via a specially crafted HTTP request.
FortiSandbox is Fortinet's security solution for detecting and analysing advanced threats. It does so by

detonating suspicious files and URLs in an isolated environment and returning verdicts. Other Fortinet products — firewalls, email security appliances, endpoint security clients, SIEMs, SOARs — depend on those verdicts to enforce blocking decisions or to trigger alerts and automated playbooks. FortiSandbox connects with those solutions through the Fortinet Security Fabric.

https://cert.gov.vu/index.php/advisories/180-advisory-169

Advisory 168: CVE-2026-56164_Microsoft SharePoint Server Missing Authentication for Critical Function Vulnerability

CVE-2026-56155 is an important-severity elevation of privilege vulnerability in Active Directory Federation Services (AD FS) caused by insufficient granularity of access control. An authorized attacker could use it to elevate privileges locally.
The vulnerability lies in an access control list on the Distributed Key Manager (DKM) container in Active Directory. If the ACL is too permissive, an authorized local attacker can read the DKM material and decrypt the private keys that protect token-signing and token-encryption certificates.

https://cert.gov.vu/index.php/advisories/179-advisory-168

Advisory 167: CVE-2026-56164_Microsoft SharePoint Server Missing Authentication for Critical Function Vulnerability

CVE-2026-56164 is a SharePoint Server flaw that Microsoft says is being exploited in attacks. It lets an unauthenticated attacker escalate privileges over the network — no credentials, no user interaction, remote.

https://cert.gov.vu/index.php/advisories/178-advisory-167

Advisory 166: CVE-2026-15410_SonicWall SMA1000 Appliances Code Injection Vulnerability CVE-2026-15409_ SonicWall SMA1000 Appliances Server-Side Request Forgery Vulnerability
CVE-2026-15409 is a critical server-side request forgery (SSRF) flaw in the SMA1000 Appliance Work Place interface, which may allow remote unauthenticated attackers to cause the appliance to make requests to unintended locations. This SSRF vulnerability in Stage 1 is used to establish access that is then leveraged to exploit the code injection vulnerability in Stage 2 (CVE-2026-15410).
CVE-2026-15410 is a post-authentication improper control of generation of code (Code Injection) vulnerability identified in the SonicWall SMA1000 Appliance Management Console (AMC), which in specific conditions could

potentially enable a remote authenticated attacker as administrator to execute arbitrary OS commands.
This vulnerability does not exist in isolation. In attacks observed so far, CVE-2026-15410 and CVE-2026-15409 are being exploited in tandem. The two vulnerabilities forma two-stage attack chain.

https://cert.gov.vu/index.php/advisories/177-cve-2026-15410-sonicwall-sma1000-appliances-code-injection-vulnerability-cve-2026-15409-sonicwall-sma1000-appliances-server-side-request-forgery-vulnerability

Advisory 165: CVE-2008-4128 — Cisco IOS Cross-Site Request Forgery Vulnerability

CVE-2008-4128 describes multiple cross-site request forgery (CSRF) vulnerabilities in the HTTP Administration component in Cisco IOS 12.4 on the 871 Integrated Services Router, allowing remote attackers to execute arbitrary commands via a certain "show privilege" command to the */level/15/exec/-* URI, and a certain "alias exec" command to the */level/15/exec/-/configure/http* URI.

https://cert.gov.vu/index.php/advisories/176-advisory-165

Advisory 164: Malware Network Infrastructure Indicators

This is not a single software vulnerability advisory, but a malware C2/network infrastructure indicator package: 3,698 IP addresses actively associated with 19 distinct malware families over a 10-day observation window (22 June – 1 July 2026). These are network indicators of compromise (IOCs) — infrastructure known to be hosting command-and-control (C2), payload delivery, or data exfiltration for active malware campaigns. CERTVU shares for cyber defense (detection/blocking) purposes only.

https://cert.gov.vu/index.php/advisories/175-advisory-164

Advisory 163: Large-Scale CMS Exploitation Campaign (Webshell Deployment)

A large-scale, globally active exploitation campaign is targeting multiple vulnerabilities across various content management systems (CMS) and their plugins. Threat actors are conducting mass scanning operations to identify vulnerable, internet-facing CMS installations and deploy webshells for persistent remote access. The campaign is notable for its scale — Five Eyes cyber agencies have flagged that AI-enabled tooling is compressing the window between vulnerability disclosure and active exploitation, meaning patch cycles

now have far less margin than before.

https://cert.gov.vu/index.php/advisories/174-advisory-163

Advisory 162: CVE-2026-56290 — Joomlack Page Builder Improper Access Control Vulnerability

Page Builder CK's front-end controller method browse.ajaxAddPicture accepts a file upload and a destination path with no authentication or authorization check at all. The only control present is a CSRF token — but that token is retrievable by anyone from the extension's own public-facing pages with a single request, so it provides no real protection against an unauthenticated attacker. The handler takes the uploaded file and a user-supplied path parameter (only trimmed, not validated) and writes the file to that attacker-chosen, web-accessible location.

https://cert.gov.vu/index.php/advisories/172-advisory-162

Advisory 161: CVE-2026-55255 — Langflow Cross-Tenant IDOR (Unauthorized Flow Execution)

An Insecure Direct Object Reference (IDOR) in Langflow's /api/v1/responses endpoint — an OpenAI-Responses-compatible API where the model field is actually a flow UUID (Langflow exposes each user's flow as a callable "model"). The vulnerable helper function, get_flow_by_id_or_endpoint_name(), resolves a flow by UUID without checking that the flow belongs to the requesting user. A separate resolution path (by endpoint name) does enforce ownership correctly — only the UUID lookup path is broken. The result: any authenticated user can execute any other user's flow simply by supplying that flow's UUID, with no authorization check in between.

https://cert.gov.vu/index.php/advisories/173-advisory-161

Advisory 160: CVE-2026-48908_SP Page Builder for Joomla_Unauthenticated File Upload RCE SP Page Builder exposes a controller task, *asset.uploadCustomIcon* (reachable via *index.php?option=com_sppagebuilder&task=asset.uploadCustomIcon*), intended to let an administrator upload a custom icon-font package. In affected versions, this endpoint performs:

- No authentication or authorization check — it's reachable by anyone, not just logged-in administrators.
- No anti-CSRF token validation.
- No server-side file-type validation on the uploaded content.

https://cert.gov.vu/index.php/advisories/170-advisory-160-1

Advisory 159: Reflected XSS — CVE-2026-48307 Vulnerability

A reflected cross-site scripting flaw.

https://cert.gov.vu/index.php/advisories/171-advisory-160

Advisory 158: Path Traversal — CVE-2026-48282, CVE-2026-48313

Improper limitation of pathnames allows access outside the intended directory scope.

https://cert.gov.vu/index.php/advisories/167-advisory-158

Advisory 157: Improper Input Validation — CVE-2026-48277, CVE-2026-48281, CVE-2026-48315

ColdFusion doesn't adequately sanitize attacker-supplied input in certain request paths.

https://cert.gov.vu/index.php/advisories/166-advisory-157

Advisory 156: Unrestricted File Upload — CVE-2026-48276, CVE-2026-48283

ColdFusion fails to properly restrict the type of files that can be uploaded through certain endpoints, allowing an attacker to upload files with dangerous extensions (e.g., executable scripts) instead of the expected data types.

https://cert.gov.vu/index.php/advisories/168-advisory-156

Advisory 155: CVE-2026-54369_Improper Link Resolution Before File Access Vulnerability

A symlink traversal vulnerability in libacl's pathname-based API functions:

- acl_get_file()
- acl_set_file()
- acl_extended_file()
- acl_delete_def_file()

These functions resolve a supplied pathname to read or write POSIX ACLs, but prior to 2.4.0 they did so without safely handling symbolic links encountered along the path. If any component of the path can be replaced with a symlink between when the caller decides on a path and when libacl actually resolves it, the operation can be redirected to a different file or directory than intended.

https://cert.gov.vu/index.php/advisories/164-advisory-155

Advisory 154: CVE-2026-57756: Contributor SQL Injection in nicen-localize-image Vulnerability

A SQL Injection vulnerability affecting the nicen-localize-image WordPress plugin, versions 1.4.9 and earlier. This is classified as a "Contributor" level vulnerability — meaning it requires an authenticated user with at least Contributor-role privileges

(WordPress's lowest privileged content-creation role) to exploit, rather than being reachable by a fully unauthenticated attacker.

https://cert.gov.vu/index.php/advisories/169-advisory-1544

Advisory 153: @fastify/express & @fastify/middie Middleware Bypass Vulnerability

1. **CVE-2026-6556** - @fastify/express Middleware Prefix Bypass - @fastify/express versions 4.0.6 and earlier only rewrite the plugin prefix for middleware mount paths when the path argument is a string. Non-string mount paths (arrays of paths and regular expressions) are left unprefixed inside prefixed plugin scopes, so middleware registered with those forms does not match the actual prefixed request path.
2. **CVE-2026-14198** - @fastify/middle Encoded Slash Bypass - @fastify/middie versions 9.1.0 through 9.3.2 decode the encoded slash (%2F) inside path parameter values before matching middleware paths, while Fastify's underlying router preserves the encoding during route lookup. The two layers disagree on the canonical request path, so the middleware fails to match a URL that the route handler does match.
3. **CVE-2026-14181** - @fastify/middie's standalone engine is vulnerable to Denial of Service via malformed percent-encoded paths. This is the same root defect class as CVE-2026-1418 (both are uncaught-exception DoS issues in the standalone engine's URL normalization), but tracked as a separate CVE ID — likely covering an overlapping or slightly different malformed-encoding trigger path.

https://cert.gov.vu/index.php/advisories/163-advisory-153

These alerts are intended for organizations, system administrators, and network administrators using the products mentioned above. The information is mainly aimed at technical users responsible for managing and securing IT systems.

Events

Cyber Month Event

October is recognized as **Cyber Month** in Vanuatu, promoting safe, responsible, and secure use of digital technology while increasing cybersecurity awareness.

As part of the **Cyber Up Pacific** campaign, CERT Vanuatu (CERTVU) leads Cyber Week activities involving schools, communities, government agencies, businesses, and other stakeholders. These activities focus on raising awareness of cyber threats, encouraging good cybersecurity practices, and helping individuals and organizations protect their information and digital systems.

Through Cyber Month activities, CERTVU supports the development of a **safer, stronger, and more resilient digital Vanuatu**.

CERT Vanuatu Efforts

CERT Vanuatu Cybersecurity Initiatives
CERT Vanuatu (CERTVU) works with national and international partners to strengthen cybersecurity awareness, skills, and resilience in Vanuatu.

Cybersecurity Awareness

CERTVU raises public awareness through radio programs, social media, and cybersecurity awareness materials.

Source: CERVTU

Multi-Stakeholder Initiatives

DCDT is developing a **Cloud Infrastructure Roadmap** and establishing a **Cybersecurity Agency** to strengthen secure digital transformation and national cybersecurity coordination.

Capacity Building

CERTVU provides cybersecurity training and skills development for government and critical infrastructure organizations.
International Collaboration: CERTVU participates in regional initiatives such as **PACSON**, supporting cybersecurity awareness, information sharing, and capacity building across the Pacific.

Incident Response

CERTVU monitors and responds to cyber incidents, helping organizations prevent, manage, and recover from cyber threats.

References

1. https://labs.watchtowr.com/enterprise-tech-in-shell-out-progress-kemp-loadmaster-uninitialized-heap-to-pre-auth-rce-cve2026-8037/
2. https://thehackernews.com/2026/06/progress-kemp-loadmaster-flaw-could-let.html
3. https://helpx.adobe.com/security/products/coldfusion/apsb26-68.html
4. https://www.catonetworks.com/blog/duneslide-two-critical-rce-vulnerabilities/
5. https://thehackernews.com/2026/07/critical-cursor-flaws-could-let-prompt.html
7. https://community.ui.com/releases/Security-Advisory-Bulletin-066-066/984eceb3-49c8-4227-942d-671c289b3afc
8. https://www.bleepingcomputer.com/news/security/sonicwall-warns-of-sma1000-flaws-exploited-in-zero-day-attacks-patchnow/
9. https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2026-0008
10. https://www.helpnetsecurity.com/2026/07/14/sonicwall-sma-attacks-via-cve-2026-15409-cve-2026-15410/
11. https://www.bleepingcomputer.com/news/security/sap-warns-of-critical-flaws-in-netweaver-and-commerce-cloud/
12. https://support.sap.com/en/my-support/knowledge-base/security-notes-news/july-2026.html
13. https://thehackernews.com/2026/07/sap-patches-cvss-99-netweaver-abap-flaw.html
14. https://www.securityweek.com/sap-patches-critical-vulnerabilities-in-netweaver-approuter-commerce-cloud/
15. https://www.securityweek.com/7-severe-vulnerabilities-patched-in-vmware-avi-load-balancer/
16. https://support.broadcom.com/web/ecx/support-content-notification/-/external/content/SecurityAdvisories/0/37926
17. https://www.bleepingcomputer.com/news/security/zoom-warns-of-critical-account-takeover-vulnerability/
18. https://www.zoom.com/en/trust/security-bulletin/zsb-26014/
19. https://www.securityweek.com/vulnerabilities-patched-by-fortinet-ivanti-servicenow/
20. https://www.securityweek.com/oracle-patches-over-1400-vulnerabilities-with-quarterly-security-updates/
21. https://www.oracle.com/security-alerts/cpujul2026.html
22. https://www.bleepingcomputer.com/news/security/arista-patches-velocloud-orchestrator-zero-day-exploited-in-attacks/
23. https://noma.security/blog/rufroot-the-mcp-bridge-vulnerability-that-turns-agents-into-rogue-admins-cve-2026-59726/
24. https://www.darkreading.com/cyber-risk/patch-resistant-rufroot-flaw-malicious-ai-agent-swarms
25. https://thehackernews.com/2026/07/ruflo-mcp-flaw-lets-unauthenticated.html
26. https://hackread.com/rufroot-vulnerability-attackers-hijack-ruflo-login/

27. https://thehackernews.com/2026/07/three-critical-vmware-flaws-allow-auth.html
28. https://www.securityweek.com/critical-vm-escape-vulnerability-patched-in-vmware-esxi/
29. https://securityaffairs.com/196231/security/broadcom-patches-critical-vmware-esxi-vulnerability-enabling-host-codeexecution.html
30. https://thehackernews.com/2026/07/critical-rails-flaw-could-let.html
31. https://darkatlas.io/blog/apt42-ai-assisted-phishing-tamecat-analysis
32. https://www.esentire.com/blog/dindoor-denorat-and-nightshadec2-analyzing-tag-150s-evolving-tradecraft
33. https://therecord.media/telegram-belarus-activist-russia-cyberattack
34. https://resident.ngo/lab/writeups/check-and-protect-analysis-of-telegram-phishing-operation-targeting-exiled-activist/
35. https://zerobec.com/blog/operation-bluedash-multi-rmm-workplace-phishing
37. https://thehackernews.com/2026/07/operation-bluedash-deploys-level-rmm.html
38. https://www.zscaler.com/blogs/security-research/helpdesk-hijackers-teams-vishing-quick-assist-and-gogrpc-backdoor
39. https://www.securityweek.com/medusahvnc-malware-uses-hidden-windows-desktops-to-evade-detection/
40. https://securityaffairs.com/196111/malware/medusahvnc-trojan-creates-hidden-desktops-to-hijack-browsers-and-stealdata.html
41. https://www.blackfog.com/medusahvnc-a-hidden-desktop/
42. https://thehackernews.com/2026/07/dysphoria-iot-botnet-adds-blockchain-c2.html
43. https://cert.gov.vu/index.php/advisories?start=42
44. https://www.facebook.com/CERTVU
45. https://www.bleepingcomputer.com/news/security/new-dysphoria-ddos-botnet-spreads-to-200k-devices-worldwide/
46. https://www.wiz.io/blog/wp2shell-cve-2026-63030-cve-2026-60137
47. https://thehackernews.com/2026/07/wordpress-wp2shell-exploitation-grows.html
48. https://www.bleepingcomputer.com/news/security/critical-wp2shell-wordpress-flaws-exploited-to-install-webshells/
49. https://www.bleepingcomputer.com/news/security/critical-servicenow-code-execution-flaw-now-exploited-in-attacks/
50. https://www.helpnetsecurity.com/2026/07/20/servicenow-cve-2026-6875-exploited/
51. https://www.bleepingcomputer.com/news/security/max-severity-adobe-coldfusion-flaw-now-exploited-in-attacks/
52. https://securityaffairs.com/194837/hacking/adobe-coldfusion-flaw-cve-2026-48282-now-exploited-in-the-wild.html
53. https://thehackernews.com/2026/07/threat-actors-probe-gitea-docker-flaw.html
54. https://cert.gov.vu/index.php/advisories

