Scottish Cyber Coordination Centre

Daily threat bulletin

27 November 2024

Vulnerabilities

Critical WordPress Anti-Spam Plugin Flaws Expose 200,000+ Sites to Remote Attacks

The Hacker News - 26 November 2024 19:53

Two critical security flaws impacting the Spam protection, Anti-Spam, and FireWall plugin WordPress could allow an unauthenticated attacker to install and enable malicious plugins on susceptible sites and potentially achieve remote code execution.The vulnerabilities, tracked as CVE-2024-10542 and CVE-2024-10781, carry a CVSS score of 9.8 out of a maximum of 10.0.

Hackers exploit critical bug in Array Networks SSL VPN products

BleepingComputer - 26 November 2024 09:26

America's cyber defense agency has received evidence of hackers actively exploiting a remote code execution vulnerability in SSL VPN products Array Networks AG and vxAG ArrayOS. [...]

Firefox and Windows zero-days exploited by Russian RomCom hackers

BleepingComputer - 26 November 2024 08:13

Russian-based RomCom cybercrime group chained two zero-day vulnerabilities in recent attacks targeting Firefox and Tor Browser users across Europe and North America. [...]

VMware Patches High-Severity Vulnerabilities in Aria Operations

SecurityWeek - 26 November 2024 15:35

The company warns that malicious hackers can craft exploits to elevate privileges or launch cross-site scripting attacks.

IBM Patches RCE Vulnerabilities in Data Virtualization Manager, Security SOAR

SecurityWeek - 26 November 2024 14:55

IBM has released patches for two high-severity remote code execution vulnerabilities in Data Virtualization Manager and Security SOAR.

Threat actors and malware

New NachoVPN attack uses rogue VPN servers to install malicious updates

BleepingComputer - 26 November 2024 18:30

A set of vulnerabilities dubbed "NachoVPN" allows rogue VPN servers to install malicious updates when unpatched Palo Alto and SonicWall SSL-VPN clients connect to them. [...]

Scottish Cyber Coordination Centre

New DDoS Campaign Exploits IoT Devices and Server Misconfigurations

Infosecurity Magazine - 26 November 2024 17:30

DDoS campaign by Matrix targets IoT devices and servers, exploiting weak credentials and public scripts

Aggressive Chinese APT Group Targets Governments with New Backdoors

Infosecurity Magazine - 26 November 2024 14:00

A Trend Micro analysis of Earth Estries found that the Chinese threat actor is using new backdoors to avoid detection during espionage operations

Incident response diplomacy: UK to launch new capability to help attacked allies

The Record from Recorded Future News - 26 November 2024 15:26

CISA and Partners Release Update to BianLian Ransomware Cybersecurity Advisory

CISA Advisories -

Today, CISA, the Federal Bureau of Investigation (FBI), and the Australian Signals Directorate's Australian Cyber Security Centre (ASD's ACSC) released updates to #StopRansomware: BianLian Ransomware Group on observed tactics, techniques, and procedures (TTPs) and indicators of compromise attributed to data extortion group, BianLian.

UK related

NHS Trust Declares Major Incident for "Cybersecurity Reasons"

Infosecurity Magazine - 26 November 2024 16:00

Wirral University Teaching Hospital has cancelled outpatient appointments as it responds to a cybersecurity incident

Software firm Blue Yonder providing services to US and UK stores, including Starbucks, hit by ransomware attack

Security Affairs - 26 November 2024 22:42

Blue Yonder, a supply chain software provider, suffered a ransomware attack, impacting operations for clients like Starbucks and grocery stores. A ransomware attack on Blue Yonder disrupted operations for several customers, including Starbucks and U.K. grocery chain Sainsbury.