Scottish Cyber Coordination Centre

Daily threat bulletin

12 August 2024

Vulnerabilities

New AMD SinkClose flaw helps install nearly undetectable malware

BleepingComputer - 09 August 2024 13:56

AMD is warning about a high-severity CPU vulnerability named SinkClose that impacts multiple generations of its EPYC, Ryzen, and Threadripper processors. The vulnerability allows attackers with Kernel-level (Ring 0) privileges to gain Ring -2 privileges and install malware that becomes nearly undetectable. [...]

Microsoft discloses unpatched Office flaw that exposes NTLM hashes

BleepingComputer - 09 August 2024 13:14

Microsoft has disclosed a high-severity vulnerability affecting Office 2016 that could expose NTLM hashes to a remote attacker. [...]

Sonos smart speakers flaw allowed to eavesdrop on users

Security Affairs - 10 August 2024 01:00

NCC Group discovered vulnerabilities in Sonos smart speakers, including a flaw that could have allowed to eavesdrop on users. Researchers from NCC Group have discovered multiple vulnerabilities in Sonos smart speakers, including a flaw, tracked as CVE-2023-50809, that could have allowed eavesdropping on users. The researchers have disclosed the vulnerabilities during the BLACK HAT USA [...]

Microsoft Reveals Four OpenVPN Flaws Leading to Potential RCE and LPE

The Hacker News - 10 August 2024 00:48

Microsoft on Thursday disclosed four medium-severity security flaws in the open-source OpenVPN software that could be chained to achieve remote code execution (RCE) and local privilege escalation (LPE).

Warnings Issued Over Cisco Device Hacking, Unpatched Vulnerabilities

SecurityWeek - 09 August 2024 11:13

CISA is warning organizations about abuse of Cisco Smart Install feature, as Cisco is notifying customers about critical phone vulnerabilities it's not patching.

CISA Adds Two Known Exploited Vulnerabilities to Catalog

CISA Advisories -

CISA has added two new vulnerabilities to its Known Exploited Vulnerabilities Catalog, based on evidence of active exploitation: CVE-2024-36971 Android Kernel Remote Code Execution Vulnerability; CVE-2024-32113 Apache OFBiz Path Traversal Vulnerability.

Threat actors and malware

EastWind Attack Deploys PlugY and GrewApacha Backdoors Using Booby-Trapped LNK Files

The Hacker News - 12 August 2024 10:13

The Russian government and IT organizations are the target of a new campaign that delivers a number of backdoors and trojans as part of a spear-phishing campaign codenamed EastWind.

New Malware Hits 300,000 Users with Rogue Chrome and Edge Extensions

The Hacker News - 10 August 2024 21:00

An ongoing, widespread malware campaign has been observed installing rogue Google Chrome and Microsoft Edge extensions via a trojan distributed via fake websites masquerading as popular software.

Threat Actors Favor Rclone, WinSCP and cURL as Data Exfiltration Tools

Infosecurity Magazine - 09 August 2024 10:00

ReliaQuest found that Rclone, WinSCP and cURL were the top three data exfiltration tools utilized by threat actors over the past year.

Cyber attacks 2024: The biggest attacks of the first half of 2024

Security Boulevard - 09 August 2024 20:45

The post Cyber attacks 2024: The biggest attacks of the first half of 2024 appeared first on Click Armor.