Scottish Cyber Coordination Centre

Daily threat bulletin

8 August 2024

Vulnerabilities

Critical XSS bug in Roundcube Webmail allows attackers to steal emails and sensitive data

Security Affairs - 07 August 2024 22:10

Researchers warn of flaws in the Roundcube webmail software that could be exploited to steal sensitive information from target accounts. Sonar's Vulnerability Research Team discovered a critical Cross-Site Scripting (XSS) vulnerability in the popular open-source webmail software Roundcube. Roundcube is included by default in the server hosting panel cPanel which has millions of installations worldwide.

Critical Security Flaw in WhatsUp Gold Under Active Attack - Patch Now

The Hacker News - 08 August 2024 11:43

A critical security flaw impacting Progress Software WhatsUp Gold is seeing active exploitation attempts, making it essential that users move quickly to apply the latest.The vulnerability in question is CVE-2024-4885 (CVSS score: 9.8), an unauthenticated remote code execution bug impacting versions of the network monitoring application released before 2023.1.3.

GhostWrite Vulnerability Facilitates Attacks on Devices With RISC-V CPU

SecurityWeek - 07 August 2024 18:00

Researchers disclose the details of GhostWrite, a RISC-V CPU vulnerability that can be exploited to gain full access to targeted devices.The post GhostWrite Vulnerability Facilitates Attacks on Devices With RISC-V CPU appeared first on SecurityWeek.

Windows Update Flaws Allow Undetectable Downgrade Attacks

SecurityWeek - 07 August 2024 16:00

Researcher showcases hack against Microsoft Windows Update architecture, turning fixed vulnerabilities into zero-days.

Chrome, Firefox Updates Patch Serious Vulnerabilities

SecurityWeek - 07 August 2024 08:50

A Chrome 127 update patches five vulnerabilities, and Firefox 129 addresses over a dozen security holes.

Threat actors and malware

Scottish Cyber Coordination Centre

New CMoon USB worm targets Russians in data theft attacks

BleepingComputer - 07 August 2024 18:23

A new self-spreading worm named 'CMoon,' capable of stealing account credentials and other data, has been distributed in Russia since early July 2024 via a compromised gas supply company website.

Cloud storage lockers from Microsoft and Google used to store and spread state-sponsored malware

The Register - 08 August 2024 02:58

Why run your own evil infrastructure when Big Tech offers robust tools hosted at trusted URLs? Black Hat State-sponsored cyber spies and criminals are increasingly using legitimate cloud services to attack their victims, according to Symantec's threat hunters who have spotted three such operations over recent months.

Ransomware in 2024: More Attacks, More Leaks, and Increased Sophistication

SecurityWeek - 07 August 2024 12:27

The ransomware scourge is still growing and still successful for attackers, Rapid7's Ransomware Radar Report 2024 shows.The post Ransomware in 2024: More Attacks, More Leaks, and Increased Sophistication appeared first on SecurityWeek.

Royal Ransomware Actors Rebrand as "BlackSuit," FBI and CISA Release Update to Advisory

CISA Advisories -

Today, CISA—in partnership with the Federal Bureau of Investigation (FBI)—released an update to joint Cybersecurity Advisory #StopRansomware: Royal Ransomware, #StopRansomware: BlackSuit (Royal) Ransomware. The updated advisory provides network defenders with recent and historically observed tactics, techniques, and procedures (TTPs) and indicators of compromise (IOCs) associated with BlackSuit and legacy Royal activity.