Scottish Cyber Coordination Centre

Daily threat bulletin

9 August 2024

Vulnerabilities

Cisco warns of critical RCE zero-days in end of life IP phones

BleepingComputer - 08 August 2024 18:27

Cisco is warning of multiple critical remote code execution zero-days in the web-based management interface of the end-of-life Small Business SPA 300 and SPA 500 series IP phones. [...]

0.0.0.0 Day flaw allows malicious websites to bypass security in major browsers

Security Affairs - 08 August 2024 19:01

An 18-year-old bug, dubbed “0.0.0.0 Day,” allows malicious websites to bypass security in Chrome, Firefox, and Safari to breach local networks. Oligo Security’s research team warns of an 18-year-old bug, dubbed “0.0.0.0 Day,” that allows malicious websites to bypass security in Chrome, Firefox, and Safari to breach local networks. The issue potentially leads to unauthorized access [...]

CISA Warns of Hackers Exploiting Legacy Cisco Smart Install Feature

The Hacker News - 09 August 2024 12:11

The U.S. Cybersecurity and Infrastructure Security Agency (CISA) has disclosed that threat actors are abusing the legacy Cisco Smart Install (SMI) feature with the aim of accessing sensitive data.The agency said it has seen adversaries “acquire system configuration files by leveraging available protocols or software on devices, such as abusing the legacy Cisco Smart Install feature.

Critical AWS Vulnerabilities Allow S3 Attack Bonanza

darkreading - 08 August 2024 13:00

Researchers at Aqua Security discovered the "Shadow Resource" attack vector and the "Bucket Monopoly" problem, where threat actors can guess the name of S3 buckets based on their public account IDs.

Windows Downgrade Attack Risks Exposing Patched Systems to Old Vulnerabilities

The Hacker News - 08 August 2024 16:35

Microsoft said it is developing security updates to address two loopholes that it said could be abused to stage downgrade attacks against the Windows update architecture and replace current versions of the operating system files with older versions. The vulnerabilities are listed below - CVE-2024-38202 (CVSS score: 7.3) - Windows Update Stack Elevation of Privilege Vulnerability ...

Scottish Cyber Coordination Centre

Threat actors and malware

SaaS Apps Present an Abbreviated Kill Chain for Attackers

darkreading - 08 August 2024 14:00

Black Hat presentation reveals adversaries don't need to complete all seven stages of a traditional kill chain to achieve their objectives.

Phishing Attack Exploits Google, WhatsApp to Steal Data

Infosecurity Magazine - 08 August 2024 14:30

The LOTS attack uses trusted sites like Google Drawings and WhatsApp to trick users into sharing data