Scottish Cyber Coordination Centre

Daily threat bulletin

5 September 2024

Vulnerabilities

Cisco fixes root escalation vulnerability with public exploit code

BleepingComputer - 04 September 2024 15:33

Cisco has fixed a command injection vulnerability in the Identity Services Engine (ISE) with public exploit code that lets attackers escalate privileges to root on vulnerable systems. [...]

Google fixed actively exploited Android flaw CVE-2024-32896

Security Affairs - 04 September 2024 23:18

Google addressed a security vulnerability in its Android operating system that is actively exploited in attacks in the wild. Google addressed a high-severity vulnerability, tracked as CVE-2024-32896 (CVSS score: 7.8), in its Android operating system that is under active exploitation in the wild.

Zyxel Patches Critical OS Command Injection Flaw in Access Points and Routers

The Hacker News - 04 September 2024 17:57

Zyxel has released software updates to address a critical security flaw impacting certain access point (AP) and security router versions that could result in the execution of unauthorized commands. Tracked as CVE-2024-7261 (CVSS score: 9.8), the vulnerability has been described as a case of operating system (OS) command injection.

Microsoft Tackling Windows Logfile Flaws With New HMAC-Based Security Mitigation

SecurityWeek - 04 September 2024 18:14

Microsoft is experimenting with a major new security mitigation to block attacks targeting flaws in the Windows Common Log File System (CLFS).

CISA Adds Three Known Exploited Vulnerabilities to Catalog

CISA Advisories -

CISA has added three new vulnerabilities to its Known Exploited Vulnerabilities Catalog, based on evidence of active exploitation. CVE-2021-20123 Draytek VigorConnect Path Traversal Vulnerability; CVE-2021-20124 Draytek VigorConnect Path Traversal VulnerabilityCVE-2024-7262 Kingsoft WPS Office Path Traversal Vulnerability.

CISA Adds One Known Exploited Vulnerability to Catalog

CISA Advisories -

CISA has added one new vulnerability to its Known Exploited Vulnerabilities Catalog, based on evidence of active exploitation. CVE-2024-7965 Google Chromium V8 Inappropriate Implementation Vulnerability.

Threat actors and malware

Hackers inject malicious JS in Cisco store to steal credit cards, credentials

BleepingComputer - 04 September 2024 12:48

Cisco's site for selling company-themed merchandise is currently offline and under maintenance due to hackers compromising it with JavaScript code that steals sensitive customer details provided at checkout. [...]

Revival Hijack supply-chain attack threatens 22,000 PyPI packages

BleepingComputer - 04 September 2024 10:43

Threat actors are utilizing an attack called "Revival Hijack," where they register new PyPi projects using the names of previously deleted packages to conduct supply chain attacks. [...]

Hackers Use Fake GlobalProtect VPN Software in New WikiLoader Malware Attack

The Hacker News - 04 September 2024 12:01

A new malware campaign is spoofing Palo Alto Networks' GlobalProtect VPN software to deliver a variant of the WikiLoader (aka WailingCrab) loader by means of a search engine optimization (SEO) campaign.

Cicada ransomware may be a BlackCat/ALPHV rebrand and upgrade

The Register - 04 September 2024 15:29

Researchers find many similarities, and nasty new customizations such as embedded compromised user credentials The Cicada3301 ransomware, which has claimed at least 20 victims since it was spotted in June, shares "striking similarities" with the notorious BlackCat ransomware.

Mallox ransomware: in-depth analysis and evolution

Securelist - 04 September 2024 11:00

In this report, we provide an in-depth analysis of the Mallox ransomware, its evolution, ransom strategy, encryption scheme, etc.

CISA and Partners Release Advisory on RansomHub Ransomware

CISA Advisories -

Today, CISA—in partnership with the Federal Bureau of Investigation (FBI), Multi-State Information Sharing and Analysis Center (MS-ISAC), and Department of Health and Human Services (HHS)—released a joint Cybersecurity Advisory, #StopRansomware: RansomHub Ransomware. This advisory provides network defenders with indicators of compromise (IOCs), tactics, techniques, and procedures (TTPs), and detection methods associated with

Scottish Cyber Coordination Centre

RansomHub activity identified through FBI investigations and third-party reporting as recently as August 2024.