Scottish Cyber Coordination Centre

Daily threat bulletin

9 October 2024

Vulnerabilities

Microsoft October 2024 Patch Tuesday fixes 5 zero-days, 118 flaws

BleepingComputer - 08 October 2024 15:16

Today is Microsoft's October 2024 Patch Tuesday, which includes security updates for 118 flaws, including five publicly disclosed zero-days, two of which are actively exploited. [...]

Three new Ivanti CSA zero-day actively exploited in attacks

Security Affairs - 08 October 2024 22:26

Software company Ivanti released security patches for three new CSA zero-day vulnerabilities actively exploited in attacks. Ivanti warned of three new security vulnerabilities (CVE-2024-9379, CVE-2024-9380, and CVE-2024-9381) in its Cloud Service Appliance (CSA) that are actively exploited in attacks in the wild.

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-2024-43047 Qualcomm Multiple Chipsets Use-After-Free Vulnerability, CVE-2024-43572 Microsoft Windows Management Console Remote Code Execution Vulnerability, and CVE-2024-43573 Microsoft Windows MSHTML Platform Spoofing Vulnerability.

Threat actors and malware

New scanner finds Linux, UNIX servers exposed to CUPS RCE attacks

BleepingComputer - 08 October 2024 18:48

An automated scanner has been released to help security professionals scan environments for devices vulnerable to the Common Unix Printing System (CUPS) RCE flaw tracked as CVE-2024-47176. [...]

New Mamba 2FA bypass service targets Microsoft 365 accounts

BleepingComputer - 08 October 2024 17:27

An emerging phishing-as-a-service (PhaaS) platform called Mamba 2FA has been observed targeting Microsoft 365 accounts in AiTM attacks using well-crafted login pages. [...]

Microsoft Detects Growing Use of File Hosting Services in Business Email Compromise Attacks

Scottish Cyber Coordination Centre

The Hacker News - 09 October 2024 10:52

Microsoft is warning of cyber attack campaigns that abuse legitimate file hosting services such as SharePoint, OneDrive, and Dropbox that are widely used in enterprise environments as a defense evasion tactic.

31 New Ransomware Groups Join the Ecosystem in 12 Months

Infosecurity Magazine - 08 October 2024 14:30

Secureworks reports a 30% increase in active ransomware groups despite law enforcement efforts, with 31 new groups emerging in the past year.

CISA and FBI Release Fact Sheet on Protecting Against Iranian Targeting of Accounts Associated with National Political Organizations

CISA Advisories -

Today, CISA and the Federal Bureau of Investigation (FBI) released joint fact sheet, How to Protect Against Iranian Targeting of Accounts Associated with National Political Organizations. This fact sheet provides information about threat actors affiliated with the Iranian Government's Islamic Revolutionary Guard Corps (IRGC) targeting and compromising accounts of Americans to stoke discord and undermine confidence in U.S. democratic institutions.