Scottish Cyber Coordination Centre

Daily threat bulletin

16 September 2024

Vulnerabilities

Windows vulnerability abused braille “spaces” in zero-day attacks

BleepingComputer - 15 September 2024 15:16

A recently fixed “Windows MSHTML spoofing vulnerability” tracked under CVE-2024-43461 is now marked as previously exploited after it was used in attacks by the Void Banshee APT hacking group. [...]

Ivanti Cloud Service Appliance flaw is being actively exploited in the wild

Security Affairs - 14 September 2024 11:30

Ivanti warned that recently patched flaw CVE-2024-8190 in Cloud Service Appliance (CSA) is being actively exploited in the wild. Ivanti warned that a newly patched vulnerability, tracked as CVE-2024-8190 (CVSS score of 7.2), in its Cloud Service Appliance (CSA) is being actively exploited.

Progress WhatsUp Gold Exploited Just Hours After PoC Release for Critical Flaw

The Hacker News - 13 September 2024 17:34

Malicious actors are likely leveraging publicly available proof-of-concept (PoC) exploits for recently disclosed security flaws in Progress Software WhatsUp Gold to conduct opportunistic attacks.

CVE-2024-28986 – SolarWinds Web Help Desk Security Vulnerability – August 2024

Security Boulevard - 14 September 2024 00:37

A critical vulnerability (CVE-2024-28986) in SolarWinds Web Help Desk puts systems at risk of exploitation, requiring immediate attention.

Threat actors and malware

Malware locks browser in kiosk mode to steal Google credentials

BleepingComputer - 14 September 2024 11:09

A malware campaign uses the unusual method of locking users in their browser’s kiosk mode to annoy them into entering their Google credentials, which are then stolen by information-stealing malware. [...]

New Linux malware called Hadooken targets Oracle WebLogic servers

Security Affairs - 13 September 2024 19:16

Scottish Cyber Coordination Centre

A new Linux malware called Hadooken targets Oracle WebLogic servers, it has been linked to several ransomware families. Aqua Security Nautilus researchers discovered a new Linux malware, called Hadooken, targeting Weblogic servers.

Cybercriminals Exploit HTTP Headers for Credential Theft via Large-Scale Phishing Attacks

The Hacker News - 16 September 2024 10:53

Cybersecurity researchers have warned of ongoing phishing campaigns that abuse refresh entries in HTTP headers to deliver spoofed email login pages that are designed to harvest users' credentials."Unlike other phishing webpage distribution behavior through HTML content, these attacks use the response header sent by a server, which occurs before the processing of the HTML content."

Apple Vision Pro Vulnerability Exposed Virtual Keyboard Inputs to Attackers

The Hacker News - 13 September 2024 20:21

Details have emerged about a now-patched security flaw impacting Apple's Vision Pro mixed reality headset that, if successfully exploited, could allow malicious attackers to infer data entered on the device's virtual keyboard.

UK related

UK Hosts International Cyber Skills Conference

Infosecurity Magazine - 16 September 2024 08:00

Nations participating in the event include the US, Canada, EU countries, India, Japan, Singapore, Ghana and Oman.