Scottish
Cyber
Coordination
Centre

Daily threat bulletin

10 July 2024

Vulnerabilities

Microsoft July 2024 Patch Tuesday fixes 142 flaws, 4 zero-days

BleepingComputer - 09 July 2024 14:52

Today is Microsoft's July 2024 Patch Tuesday, which includes security updates for 142 flaws, including two actively exploited and two publicly disclosed zero-days.

New OpenSSH Vulnerability Discovered: Potential Remote Code Execution Risk

The Hacker News - 10 July 2024 09:56

Select versions of the OpenSSH secure networking suite are susceptible to a new vulnerability that can trigger remote code execution (RCE). The vulnerability, tracked as CVE-2024-6409 (CVSS score: 7.0), is distinct from CVE-2024-6387 (aka RegreSSHion) and relates to a case of code execution in the privsep child process due to a race condition in signal handling. It only impacts versions 8.7p1.

RADIUS Protocol Vulnerability Exposes Networks to MitM Attacks

The Hacker News - 09 July 2024 19:09

Cybersecurity researchers have discovered a security vulnerability in the RADIUS network authentication protocol called BlastRADIUS that could be exploited by an attacker to stage Mallory-in-the-middle (MitM) attacks and bypass integrity checks under certain circumstances. The RADIUS protocol allows certain Access-Request messages to have no integrity or authentication checks.

Hackers Exploiting Jenkins Script Console for Cryptocurrency Mining Attacks

The Hacker News - 09 July 2024 18:20

Cybersecurity researchers have found that it's possible for attackers to weaponize improperly configured Jenkins Script Console instances to further criminal activities such as cryptocurrency mining. Misconfigurations such as improperly set up authentication mechanisms expose the '/script' endpoint to attackers.

SAP Patches High-Severity Vulnerabilities in PDCE, Commerce

SecurityWeek - 09 July 2024 14:32

Patch Tuesday: Enterprise software vendor SAP releases patches for high-severity vulnerabilities in multiple products and tools.

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-2024-23692 Rejetto HTTP File Server Improper Neutralization of Special Elements Used in a Template Engine Vulnerability CVE-2024-38080 Microsoft Windows Hyper-V Privilege Escalation Vulnerability CVE-2024-38112 Microsoft Windows MSHTML Platform Spoofing Vulnerability.

Threat actors and malware

Chinese APT40 hackers hijack SOHO routers to launch attacks

BleepingComputer - 09 July 2024 12:11

An advisory by CISA and multiple international cybersecurity agencies highlights the tactics, techniques, and procedures (TTPs) of APT40 (aka "Kryptonite Panda"), a state-sponsored Chinese cyber-espionage actor. [...]

ViperSoftX Malware Disguises as eBooks on Torrents to Spread Stealthy Attacks

The Hacker News - 10 July 2024 12:05

The sophisticated malware known as ViperSoftX has been observed being distributed as eBooks over torrents."A notable aspect of the current variant of ViperSoftX is that it uses the Common Language Runtime (CLR) to dynamically load and run PowerShell commands, thereby creating a PowerShell environment within AutoIt for operations," Trellix security researchers Mathanraj Thangaraju and Sijo Jacob

Eldorado Ransomware Cruises Onto the Scene to Target VMware ESXi

darkreading - 09 July 2024 17:37

The ransomware-as-a-service platform just rolled off the assembly line, also targets Windows, and uses Golang for cross-platform capabilities.

Trojanized jQuery Packages Spread via 'Complex' Supply Chain Attack

darkreading - 09 July 2024 17:06

The campaign, which distributes dozens of malicious jQuery variants across npm, GitHub, and jsDelivr, appears to be a manual effort, and lacks the typical pattern that characterizes similar, related attacks.