Scottish
Cyber
Coordination
Centre

Daily threat bulletin

10 September 2024

Vulnerabilities

Critical SonicWall SSLVPN bug exploited in ransomware attacks

BleepingComputer - 09 September 2024 18:50

Ransomware affiliates exploit a critical security vulnerability in SonicWall SonicOS firewall devices to breach victims' networks. [...]

Progress Software Issues Patch for Vulnerability in LoadMaster and MT Hypervisor

The Hacker News - 09 September 2024 15:54

Progress Software has released security updates for a maximum-severity flaw in LoadMaster and Multi-Tenant (MT) hypervisor that could result in the execution of arbitrary operating system commands.

Akira Ransomware Actors Exploit SonicWall Bug for RCE

darkreading - 09 September 2024 21:39

CISA has added CE-2024-40766 to its Known Exploited Vulnerabilities catalog.

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-2016-3714 ImageMagick Improper Input Validation Vulnerability; CVE-2017-1000253 Linux Kernel PIE Stack Buffer Corruption Vulnerability; CVE-2024-40766 SonicWall SonicOS Improper Access Control Vulnerability.

Threat actors and malware

Quad7 botnet targets more SOHO and VPN routers, media servers

BleepingComputer - 09 September 2024 18:30

The Quad7 botnet is expanding its targeting scope with the addition of new clusters and custom implants that now also target Zyxel VPN appliances and Ruckus wireless routers. [...]

Chinese Hackers Exploit Visual Studio Code in Southeast Asian Cyberattacks

The Hacker News - 09 September 2024 18:46

The China-linked advanced persistent threat (APT) group known as Mustang Panda has been observed weaponizing Visual Studio Code software as part of espionage operations targeting government entities in Southeast Asia."This threat actor used Visual Studio Code's embedded reverse shell feature to gain a foothold in target networks."

New Android SpyAgent Malware Uses OCR to Steal Crypto Wallet Recovery Keys

The Hacker News - 09 September 2024 15:20

Android device users in South Korea have emerged as a target of a new mobile malware campaign that delivers a new type of threat dubbed SpyAgent. The malware "targets mnemonic keys by scanning for images on your device that might contain them," McAfee Labs researcher SangRyol Ryu said in an analysis, adding the targeting footprint has broadened in scope to include the U.K.

TfL Admits Some Services Are Down Following Cyber-Attack

Infosecurity Magazine - 09 September 2024 09:30

Transport for London has revealed several digital services are suspended after a cyber-attack last week.