Scottish Cyber Coordination Centre

Daily threat bulletin

9 April 2024

Vulnerabilities

Critical RCE bug in 92,000 D-Link NAS devices now exploited in attacks

BleepingComputer - 08 April 2024 19:17

Attackers are now actively targeting over 92,000 end-of-life D-Link Network Attached Storage (NAS) devices exposed online and unpatched against a critical remote code execution (RCE) zero-day flaw. [...]

Confidential VMs Hacked via New Ahoi Attacks

SecurityWeek - 08 April 2024 14:16

New Ahoi attacks Heckler and WeSee target AMD SEV-SNP and Intel TDX with malicious interrupts to hack confidential VMs.The post Confidential VMs Hacked via New Ahoi Attacks appeared first on SecurityWeek.

Thousands of Ivanti VPN Appliances Impacted by Recent Vulnerability

SecurityWeek - 08 April 2024 15:41

Researchers at the Shadowserver Foundation identify thousands of internet-exposed Ivanti VPN appliances likely impacted by a recently disclosed vulnerability leading to remote code execution.The post Thousands of Ivanti VPN Appliances Impacted by Recent Vulnerability appeared first on SecurityWeek.

CISA Adds Two Known Exploited Vulnerabilities to Catalog

CISA Advisories -

CISA has added two new vulnerabilities to its Known Exploited Vulnerabilities Catalog, based on evidence of active exploitation. CVE-2024-29748 Android Pixel Privilege Escalation Vulnerability. These types of vulnerabilities are frequent attack vectors for malicious cyber actors and pose significant risks to the federal enterprise.

Threat actors and malware

Solar Spider Spins Up New Malware to Entrap Saudi Arabian Financial Firms

Scottish Cyber Coordination Centre

darkreading - 08 April 2024 07:00

An ongoing cyberattack campaign with apparent ties to China uses a new version of sophisticated JavaScript remote access Trojan JSOutProx and is now targeting banks in the Middle East.

New Malware “Latrodectus” Linked to IcedID

Infosecurity Magazine - 08 April 2024 16:30

The malware, discovered by Proofpoint and Team Cymru, was mainly utilized by initial access brokers