Scottish Cyber Coordination Centre

Daily threat bulletin

14 November 2024

Vulnerabilities

Critical bug in EoL D-Link NAS devices now exploited in attacks

BleepingComputer - 13 November 2024 14:36

Attackers now target a critical severity vulnerability with publicly available exploit code that affects multiple models of end-of-life D-Link network-attached storage (NAS) devices. [...]

Microsoft patches Windows zero-day exploited in attacks on Ukraine

BleepingComputer - 13 November 2024 17:33

Suspected Russian hackers were caught exploiting a recently patched Windows vulnerability as a zero-day in ongoing attacks targeting Ukrainian entities. [...]

High-Severity Vulnerabilities Patched in Zoom, Chrome

SecurityWeek - 13 November 2024 12:45

Zoom Apps security updates resolve six vulnerabilities and Chrome 131 stable is rolling out with 12 security fixes.

Citrix, Fortinet Patch High-Severity Vulnerabilities

SecurityWeek - 13 November 2024 12:00

Citrix and Fortinet have released patches for multiple vulnerabilities, including high-severity bugs in NetScaler and FortiOS.

Ivanti Patches 50 Vulnerabilities Across Several Products

SecurityWeek - 13 November 2024 13:39

Ivanti has released fixes for dozens of vulnerabilities in Endpoint Manager, Avalanche, Connect Secure, Policy Secure, and Secure Access Client.

OvrC Platform Vulnerabilities Expose IoT Devices to Remote Attacks and Code Execution

The Hacker News - 13 November 2024 15:58

A security analysis of the OvrC cloud platform has uncovered 10 vulnerabilities that could be chained to allow potential attackers to execute code remotely on connected devices.

Threat actors and malware

Bitdefender released a decryptor for the ShrinkLocker ransomware

Scottish Cyber Coordination Centre

Security Affairs - 14 November 2024 01:05

Bitdefender released a decryptor for the ShrinkLocker ransomware, which modifies BitLocker configurations to encrypt a system's drives. ShrinkLocker ransomware was first discovered in May 2024 by researchers from Kaspersky.

Russian Hackers Exploit New NTLM Flaw to Deploy RAT Malware via Phishing Emails

The Hacker News - 14 November 2024 12:13

A newly patched security flaw impacting Windows NT LAN Manager (NTLM) was exploited as a zero-day by a suspected Russia-linked actor as part of cyber attacks targeting Ukraine. The vulnerability in question, CVE-2024-43451 (CVSS score: 6.5), refers to an NTLM hash disclosure spoofing vulnerability that could be exploited to steal a user's NTLMv2 hash.

Hamas-Affiliated WIRTE Employs SameCoin Wiper in Disruptive Attacks Against Israel

The Hacker News - 13 November 2024 22:39

A threat actor affiliated with Hamas has expanded its malicious cyber operations beyond espionage to carry out disruptive attacks that exclusively target Israeli entities.The activity, linked to a group called WIRTE, has also targeted the Palestinian Authority, Jordan, Iraq, Saudi Arabia, and Egypt, Check Point said in an analysis.

Hive0145 Targets Europe with Advanced Strela Stealer Campaigns

Infosecurity Magazine - 13 November 2024 19:00

Hive0145 is targeting Spain, Germany, Ukraine with Strela Stealer malware in invoice phishing tactic

OpenText Cybersecurity Unveils 2024's Nastiest Malware

darkreading - 13 November 2024 23:46