Scottish Cyber Coordination Centre

Daily threat bulletin

26 August 2024

Vulnerabilities

Patch Now: Second SolarWinds Critical Bug in Web Help Desk

darkreading - 23 August 2024 19:38

The disclosure of CVE-2024-28987 means that, in two weeks, there have been two critical bugs and corresponding patches for SolarWinds' less-often-discussed IT help desk software.

CISA Urges Federal Agencies to Patch Versa Director Vulnerability by September

The Hacker News - 24 August 2024 13:33

The U.S. Cybersecurity and Infrastructure Security Agency (CISA) has placed a security flaw impacting Versa Director to its Known Exploited Vulnerabilities (KEV) catalog based on evidence of active exploitation. The medium-severity vulnerability, tracked as CVE-2024-39717 (CVSS score: 6.6), is case of file upload bug impacting the "Change Favicon" feature.

Secure Web Gateway Vulnerabilities Exposed: SquareX's Research Stirs the Industry

Security Boulevard - 26 August 2024 03:07

At DEF CON 32 this year, SquareX presented compelling research that revealed the shortcomings of Secure Web Gateways (SWG) in protecting the browser and demonstrated 30+ foolproof methods to bypass them.

Threat actors and malware

Stealthy 'sedexp' Linux malware evaded detection for two years

BleepingComputer - 24 August 2024 11:36

A stealthy Linux malware named 'sedexp' has been evading detection since 2022 by using a persistence technique not yet included in the MITRE ATT&CK framework.

New malware Cthulhu Stealer targets Apple macOS users

Security Affairs - 23 August 2024 09:25

Cato Security found a new info stealer, called Cthulhu Stealer, that targets Apple macOS and steals a wide range of information. Cado Security researchers have discovered a malware-as-a-service (MaaS) targeting macOS users dubbed Cthulhu Stealer. Cthulhu Stealer targets macOS users via an Apple disk image (DMG) that disguises itself as legitimate software.

Hackers now use AppDomain Injection to drop CobaltStrike beacons

BleepingComputer - 23 August 2024 13:31

Scottish Cyber Coordination Centre

A wave of attacks that started in July 2024 rely on a less common technique called AppDomain Manager Injection, which can weaponize any Microsoft .NET application on Windows. [...]

New Android Malware NGate Steals NFC Data to Clone Contactless Payment Cards

The Hacker News - 26 August 2024 11:16

Cybersecurity researchers have uncovered new Android malware that can relay victims' contactless payment data from physical credit and debit cards to an attacker-controlled device with the goal of conducting fraudulent operations.The Slovak cybersecurity company is tracking the novel malware as NGate, stating it observed the crimeware campaign targeting three banks in Czechia.The malware "has

New Qilin Ransomware Attack Uses VPN Credentials, Steals Chrome Data

The Hacker News - 23 August 2024 16:54

The threat actors behind a recently observed Qilin ransomware attack have stolen credentials stored in Google Chrome browsers on a small set of compromised endpoints.The use of credential harvesting in connection with a ransomware infection marks an unusual twist, and one that could have cascading consequences, cybersecurity firm Sophos said in a Thursday report.

Constantly Evolving MoonPeak RAT Linked to North Korean Spying

darkreading - 23 August 2024 21:46

The malware is a customized variant of the powerful open source XenoRAT information stealing malware often deployed by Kimsuky and other DPRK APTs.