Scottish Cyber Coordination Centre

Daily Threat Bulletin

06 December 2024

Vulnerabilities

Critical Mitel MiCollab Flaw Exposes Systems to Unauthorized File and Admin Access

The Hacker News - 05 December 2024 21:26

Cybersecurity researchers have released a proof-of-concept (PoC) exploit that strings together a now-patched critical security flaw impacting Mitel MiCollab with an arbitrary file read zero-day, granting an attacker the ability to access files from susceptible instances.

Critical Vulnerability Discovered in SailPoint IdentityIQ

SecurityWeek - 06 December 2024 06:50

A critical directory traversal vulnerability in the SailPoint IdentityIQ IAM platform exposes restricted files to attackers.

Hundred of CISCO switches impacted by bootloader flaw

Security Affairs - 06 December 2024 01:46

A bootloader vulnerability in Cisco NX-OS affects 100+ switches, allowing attackers to bypass image signature checks. Cisco released security patches for a vulnerability, tracked as CVE-2024-20397 (CVSS score of 5.2), in the NX-OS software's bootloader that could be exploited by attackers to bypass image signature verification.

Threat actors and malware

Latrodectus malware and how to defend against it with Wazuh

BleepingComputer - 05 December 2024 11:02

Latrodectus is a versatile malware family that infiltrate systems, steal sensitive data, and evades detection. Learn more from Wazuh about Latrodectus malware and how to defend against it using the open-source XDR.

Russia's 'BlueAlpha' APT Hides in Cloudflare Tunnels

darkreading - 05 December 2024 23:04

Cloudflare Tunnels is just the latest legitimate cloud service that cybercriminals and state-sponsored threat actors are abusing to hide their tracks.

Russia-linked APT Secret Blizzard spotted using infrastructure of other threat actors

Security Affairs - 05 December 2024 10:17

Researchers from Microsoft Threat Intelligence collected evidence that Russia-linked APT group Secret Blizzard has used the tools and infrastructure of at least 6 other threat actors during the past 7 years.

Scottish Cyber Coordination Centre

US arrests Scattered Spider suspect linked to telecom hacks

BleepingComputer - 05 December 2024 16:31

U.S. authorities have arrested a 19-year-old teenager linked to the notorious Scattered Spider cybercrime gang who is now charged with breaching a U.S. financial institution and two unnamed telecommunications firms.

UK incidents

British hospitals hit by cyberattacks still battling to get systems back online

The Register - 05 December 2024 13:25

Children's hospital and cardiac unit say criminals broke in via shared 'digital gateway service'. Both National Health Service trusts that oversee the various hospitals hit by separate cyberattacks last week have confirmed they're still in the process of restoring systems.

BT Group confirms attackers tried to break into Conferencing division

The Register - 05 December 2024 12:03

Sensitive data allegedly stolen from US subsidiary following Black Basta post. BT Group confirmed it is dealing with an attempted attack on one of its legacy business units after the Black Basta ransomware group claimed compromise.

Operation Destabilise dismantled Russian money laundering networks

Security Affairs - 05 December 2024 16:09

The U.K. National Crime Agency (NCA) disrupted Russian money laundering networks linked to organized crime across the U.K., Middle East, Russia, and South America as part of an operation called Operation Destabilise.