Scottish Cyber Coordination Centre

Daily threat bulletin

11 December 2024

Vulnerabilities

Microsoft Fixes 72 Flaws, Including Patch for Actively Exploited CLFS Vulnerability

The Hacker News - 11 December 2024 13:46

Microsoft closed out its Patch Tuesday updates for 2024 with fixes for a total of 72 security flaws spanning its software portfolio, including one that it said has been exploited in the wild.Of the 72 flaws, 17 are rated Critical, 54 are rated Important, and one is rated Moderate in severity.

Ivanti warns of maximum severity CSA auth bypass vulnerability

BleepingComputer - 10 December 2024 15:40

Ivanti warned customers on Tuesday about a new maximum-severity authentication bypass vulnerability in its Cloud Services Appliance (CSA) solution. [...]

Cisco Says Flaws in Industrial Routers, BGP Tool Remain Unpatched 8 Months After Disclosure

SecurityWeek - 10 December 2024 13:19

Cisco Talos has disclosed the details of apparently unpatched vulnerabilities in MC Technologies industrial routers and the GoCast BGP tool.

SAP fixed critical SSRF flaw in NetWeaver's Adobe Document Services

Security Affairs - 10 December 2024 16:35

SAP has issued patches for 16 vulnerabilities, including a critical SSRF flaw in NetWeaver's Adobe Document Services. SAP addressed 16 vulnerabilities as part of its December 2024 Security Patch Day.

New Cleo zero-day RCE flaw exploited in data theft attacks

BleepingComputer - 10 December 2024 11:09

Hackers are actively exploiting a zero-day vulnerability in Cleo managed file transfer software to breach corporate networks and conduct data theft attacks. [...]

Adobe Patches Over 160 Vulnerabilities Across 16 Products

SecurityWeek - 10 December 2024 19:58

Adobe has patched over 160 vulnerabilities across over a dozen products, including Reader, Illustrator, Photoshop and Connect.

Scottish Cyber Coordination Centre

Threat actors and malware

New AppLite Malware Targets Banking Apps in Phishing Campaign

Infosecurity Magazine - 10 December 2024 15:00

New AppLite Banker malware targets Android devices, employing advanced phishing techniques to steal credentials and data

Hackers Weaponize Visual Studio Code Remote Tunnels for Cyber Espionage

The Hacker News - 10 December 2024 17:30

A suspected China-nexus cyber espionage group has been attributed to an attacks targeting large business-to-business IT service providers in Southern Europe as part of a campaign codenamed Operation Digital Eye.

Hackers Exploit AWS Misconfigurations in Massive Data Breach

Infosecurity Magazine - 10 December 2024 17:30

Hackers exploited AWS misconfigurations, leaking 2TB of sensitive data, including customer information, credentials and proprietary source code

Inside the incident: Uncovering an advanced phishing attack

BleepingComputer - 10 December 2024 11:01

Recently, Varonis investigated a phishing campaign in which a malicious email enabled a threat actor to access the organization.

Ongoing Phishing and Malware Campaigns in December 2024

The Hacker News - 10 December 2024 16:31

Cyber attackers never stop inventing new ways to compromise their targets. That's why organizations must stay updated on the latest threats.

2024 saw a 30% increase in active ransomware groups

Security Magazine - 11 December 2024 01:00

2024 saw a rise in ransomware activity.

Scottish Parliament TV at Risk From Deepfakes

darkreading - 10 December 2024 18:51

Because the streaming service website offers no content restrictions, attackers are able to hijack and manipulate live streams.