Scottish Cyber Coordination Centre

Daily threat bulletin

19 July 2024

Vulnerabilities

SolarWinds fixes 8 critical bugs in access rights audit software

BleepingComputer - 18 July 2024 12:51

SolarWinds has fixed eight critical vulnerabilities in its Access Rights Manager (ARM) software, six of which allowed attackers to gain remote code execution (RCE) on vulnerable devices.

Microsoft fixes bug blocking Windows 11 Photos from starting

BleepingComputer - 18 July 2024 11:38

Microsoft has fixed a known issue preventing the Microsoft Photos app from starting on some Windows 11 22H2 and 23H2 systems.

Critical Cisco bug lets hackers add root users on SEG devices

BleepingComputer - 18 July 2024 09:48

Cisco has fixed a critical severity vulnerability that lets attackers add new users with root privileges and permanently crash Security Email Gateway (SEG) appliances using emails with malicious attachments.

SAPwned flaws in SAP AI core could expose customers' data

Security Affairs - 18 July 2024 15:18

Researchers discovered security flaws in SAP AI Core cloud-based platform that could expose customers data. Cybersecurity researchers at Wiz uncovered five security flaws, collectively tracked as SAPwned, in the SAP AI Core cloud-based platform. An attacker can exploit the flaws to obtain access tokens and customer data.

Threat actors and malware

Revolver Rabbit gang registers 500,000 domains for malware campaigns

BleepingComputer - 18 July 2024 18:30

A cybercriminal gang that researchers track as Revolver Rabbit has registered more than 500,000 domain names for infostealer campaigns that target Windows and macOS systems.

TAG-100: New Threat Actor Uses Open-Source Tools for Widespread Attacks

The Hacker News - 18 July 2024 15:40

Unknown threat actors have been observed leveraging open-source tools as part of a suspected cyber espionage campaign targeting global government and private sector

organizations. Recorded Future's Insikt Group is tracking the activity under the temporary moniker TAG-100, noting that the adversary likely compromised organizations in at least ten countries.

Chinese Hacking Group APT41 Infiltrates Global Shipping and Tech Sectors, Mandiant Warns

SecurityWeek - 18 July 2024 18:46

Researchers at Mandiant are flagging a significant resurgence in malware attacks by APT41, a prolific Chinese government-backed hacking team caught breaking into organizations in the shipping, logistics, technology, and automotive sectors in Europe and Asia.

UK related

UK Government Set to Introduce New Cyber Security and Resilience Bill

Infosecurity Magazine - 18 July 2024 09:30

A new UK Cyber Security and Resilience Bill will update the NIS Regulations.