Scottish Cyber Coordination Centre

Daily Threat Bulletin

9 May 2025

Vulnerabilities

Cisco fixes max severity IOS XE flaw letting attackers hijack devices

BleepingComputer - 08 May 2025 17:53

Cisco has fixed a maximum severity flaw in IOS XE Software for Wireless LAN Controllers by a hard-coded JSON Web Token (JWT) that allows an unauthenticated remote attacker to take over devices.

SonicWall Patches 3 Flaws in SMA 100 Devices Allowing Attackers to Run Code as Root

The Hacker News - 08 May 2025 20:26

SonicWall has released patches to address three security flaws affecting SMA 100 Secure Mobile Access (SMA) appliances that could be fashioned to result in remote code execution.

Improperly Patched Samsung MagicINFO Vulnerability Exploited by Botnet

SecurityWeek - 08 May 2025 11:44

The patches for an exploited Samsung MagicINFO vulnerability are ineffective and a Mirai botnet has started targeting it.

Threat actors and malware

Russia-Linked APT Star Blizzard Uses ClickFix to Deploy New LostKeys Malware, Google Warns

SecurityWeek - 08 May 2025 12:55

Russia-linked APT Star Blizzard is using the ClickFix technique in recent attacks distributing the LostKeys malware.

Malicious PyPi package hides RAT malware, targets Discord devs since 2022

BleepingComputer - 08 May 2025 15:51

A malicious Python package targeting Discord developers with remote access trojan (RAT) malware was spotted on the Python Package Index (PyPI) after more than three years.

Scottish Cyber Coordination Centre

Qilin Ransomware Ranked Highest in April 2025 with 72 Data Leak Disclosures

The Hacker News - 08 May 2025 20:17

Threat actors with ties to the Qilin ransomware family have leveraged malware known as SmokeLoader along with a previously undocumented .NET compiled loader codenamed NETXLOADER as part of a campaign observed in November 2024.

Hacker Finds New Technique to Bypass SentinelOne EDR Solution

Infosecurity Magazine - 08 May 2025 09:00

Security researchers at Aon have discovered a threat actor who bypassed SentinelOne EDR protection to deploy Babuk ransomware.

UK Specific

UK Cyber Essentials Certification Numbers Falling Short

Infosecurity Magazine - 08 May 2025 12:20

The UK government is set to prioritize increasing the number of UK organizations who are Cyber Essentials certified over the coming year

UK Launches New Cybersecurity Assessment Initiatives to Drive Secure by Design

Infosecurity Magazine - 08 May 2025 11:15

The UK government unveiled two new assessment schemes to boost confidence in the security of products and services during CYBERUK

Marks & Spencer Hackers Tricked IT Workers Into Resetting Passwords

Security Magazine - 08 May 2025 13:00

More information on the cyberattacks against Marks & Spencer (M&S) and Co-op has emerged, revealing that hackers deceived IT workers into resetting passwords