Scottish Cyber Coordination Centre

Daily Threat Bulletin

22 April 2025

Vulnerabilities

Critical Erlang/OTP SSH RCE bug now has public exploits, patch now

BleepingComputer - 19 April 2025 11:05

Public exploits are now available for a critical Erlang/OTP SSH vulnerability tracked as CVE-2025-32433, allowing unauthenticated attackers to remotely execute code on impacted devices. [...]

ASUS Confirms Critical Flaw in AiCloud Routers; Users Urged to Update Firmware

The Hacker News - 19 April 2025 15:22

ASUS has disclosed a critical security flaw impacting routers with AiCloud enabled that could permit remote attackers to perform unauthorized execution of functions on susceptible devices.The vulnerability, tracked as CVE-2025-2492, has a CVSS score of 9.2 out of a maximum of 10.0."An improper authentication control vulnerability exists in certain ASUS router firmware series,"

Threat actors and malware

Phishers abuse Google OAuth to spoof Google in DKIM replay attack

BleepingComputer - 20 April 2025 14:31

In a rather clever attack, hackers leveraged a weakness that allowed them to send a fake email that seemed delivered from Google's systems, passing all verifications but pointing to a fraudulent page that collected logins. [...]

State-sponsored hackers embrace ClickFix social engineering tactic

BleepingComputer - 20 April 2025 11:14

ClickFix attacks are being increasingly adopted by threat actors of all levels, with researchers now seeing multiple advanced persistent threat (APT) groups from North Korea, Iran, and Russia utilizing the tactic to breach networks. [...]

Kimsuky APT exploited BlueKeep RDP flaw in attacks against South Korea and Japan

Security Affairs - 21 April 2025 19:25

Researchers spotted a new North Korea-linked group Kimsuky 's campaign, exploiting a patched Microsoft Remote Desktop Services flaw to gain initial access. While investigating a security breach, the AhnLab SEcurity intelligence Center (ASEC) researchers discovered a North Korea-linked group Kimsuky 's campaign, tracked as Larva-24005. Attackers exploited an RDP vulnerability to gain initial access to [...]

Scottish Cyber Coordination Centre

New sophisticate malware SuperCard X targets Androids via NFC relay attacks

Security Affairs - 21 April 2025 10:24

'SuperCard X' – a new MaaS – targets Androids via NFC relay attacks, enabling fraudulent POS and ATM transactions with stolen card data. Cleafy researchers discovered a new malware-as-a-service (MaaS) called SuperCard X targeting Android devices with NFC relay attacks for fraudulent cash-outs. Attackers promote the MaaS through Telegram channels, analysis shows SuperCard X builds [...]

Attackers exploited SonicWall SMA appliances since January 2025

Security Affairs - 19 April 2025 18:37

Threat actors are actively exploiting a remote code execution flaw in SonicWall Secure Mobile Access (SMA) appliances since January 2025. Arctic Wolf researchers warn that threat actors actively exploit a vulnerability, tracked as CVE-2021-20035 (CVSS score of 7.1), in SonicWall Secure Mobile Access (SMA) since at least January 2025. The vulnerability is an OS Command [...]