Scottish
Cyber
Coordination
Centre

Daily threat bulletin

26 November 2024

Vulnerabilities

QNAP addresses critical flaws across NAS, router software

BleepingComputer - 25 November 2024 18:13

QNAP has released security bulletins over the weekend, which address multiple vulnerabilities, including three critical severity flaws that users should address as soon as possible. […]

CISA Urges Agencies to Patch Critical “Array Networks” Flaw Amid Active Attacks

The Hacker News - 26 November 2024 11:33

The U.S. Cybersecurity and Infrastructure Security Agency (CISA) on Monday added a now-patched critical security flaw impacting Array Networks AG and vxAG secure access gateways to its Known Exploited Vulnerabilities (KEV) catalog following reports of active exploitation in the wild.

Recent Zyxel Firewall Vulnerability Exploited in Ransomware Attacks

SecurityWeek - 25 November 2024 18:50

A ransomware group has been observed exploiting a recently patched command injection vulnerability in Zyxel firewalls for initial access.

Vulnerabilities Expose mySCADA myPRO Systems to Remote Hacking

SecurityWeek - 25 November 2024 17:00

Critical vulnerabilities patched by mySCADA in its myPRO HMI/SCADA product can allow remote and unauthenticated takeover of the system.

Threat actors and malware

Malware campaign abused flawed Avast Anti-Rootkit driver

Security Affairs - 25 November 2024 14:50

Threat actors exploit an outdated Avast Anti-Rootkit driver to evade detection, disable security tools, and compromise the target systems. Trellix researchers uncovered a malware campaign that abused a vulnerable Avast Anti-Rootkit driver (aswArPot.sys) to gain deeper access to the target system, disable security solutions, and gain system control.

Salt Typhoon hackers backdoor telcos with new GhostSpider malware

BleepingComputer - 25 November 2024 12:12

The Chinese state-sponsored hacking group Salt Typhoon has been observed utilizing a new “GhostSpider” backdoor in attacks against telecommunication service providers. [...]

BlackBasta Ransomware Brand Picks Up Where Conti Left Off

darkreading - 25 November 2024 22:25

New analysis says law enforcement efforts against Russian-language ransomware-as-a-service (RaaS) infrastructure helped consolidate influence behind BlackBasta, but some experts aren’t so sure the brand means that much.

Fancy Bear ‘Nearest Neighbor’ Attack Uses Nearby Wi-Fi Network

darkreading - 25 November 2024 19:18

In a "new class of attack," the Russian APT breached a target in Washington, DC, by credential-stuffing wireless networks in close proximity to it and daisy-chaining a vector together in a resourceful and creative way, according to researchers.

UK related

Russia-linked threat actors threaten the UK and its allies, minister to say

Security Affairs - 25 November 2024 09:20

A senior UK minister will warn that Russia is preparing cyberattacks against the UK and its allies to undermine support for Ukraine. Russia may launch cyberattacks against the UK and its allies in retaliation for their support of Ukraine, Chancellor of the Duchy of Lancaster Pat McFadden is expected to state during a NATO meeting. [...]

Blue Yonder ransomware attack disrupts grocery store supply chain

BleepingComputer - 25 November 2024 17:11

Supply chain management firm Blue Yonder is warning that a ransomware attack caused significant disruption to its services, with the outages impacting grocery store chains in the UK. [...]