Scottish Cyber Coordination Centre

Daily Threat Bulletin

28 February 2025

Vulnerabilities

Cisco Patches Vulnerabilities in Nexus Switches

SecurityWeek - 27 February 2025 12:57

Cisco has patched command injection and DoS vulnerabilities affecting some of its Nexus switches, including a high-severity flaw.

MITRE Caldera security advisory warns of maximum severity flaw

Security Magazine - 27 February 2025 13:00

MITRE Caldera security advisory warns of maximum severity flaw, and experts weigh share their insights.

Threat actors and malware

DragonForce Ransomware group is targeting Saudi Arabia

Security Affairs - 27 February 2025 10:10

DragonForce ransomware has recently been reported to target organizations in the Kingdom of Saudi Arabia (KSA). A significant incident identified by Resecurity involved a data leak from a prominent real estate and construction company in Riyadh.

Winos 4.0 Malware Targets Taiwan With Email Impersonation

Infosecurity Magazine - 27 February 2025 17:00

A new malware campaign using Winos 4.0 that targets organizations in Taiwan through email impersonation has been uncovered by cybersecurity experts.

Vo1d malware botnet grows to 1.6 million Android TVs worldwide

BleepingComputer - 27 February 2025 18:49

A new variant of the Vo1d malware botnet has grown to 1,590,299 infected Android TV devices across 226 countries, recruiting devices as part of anonymous proxy server networks.

Chinese APT Uses VPN Bug to Exploit Worldwide OT Orgs

darkreading - 27 February 2025 15:29

Companies critical to the aviation and aerospace supply chains didn't patch a known CVE, providing opportunity for foreign espionage.

Scottish Cyber Coordination Centre

26 New Threat Groups Spotted in 2024: CrowdStrike

SecurityWeek - 27 February 2025 20:03

CrowdStrike has published its 2025 Global Threat Report, which warns of faster breakout time and an increase in Chinese activity.