Scottish
Cyber
Coordination
Centre

Daily Threat Bulletin

17 March 2025

Vulnerabilities

Cisco IOS XR flaw allows attackers to crash BGP process on routers

Security Affairs - 15 March 2025 11:41

Cisco addressed a denial of service (DoS) vulnerability that allows attackers to crash the Border Gateway Protocol (BGP) process on IOS XR routers. Cisco has addressed a denial of service (DoS) vulnerability, tracked as CVE-2025-20115, that could allow an unauthenticated, remote attacker to crash the Border Gateway Protocol (BGP) process on IOS XR routers by sending a single BGP [...]

3 Ivanti flaws added to CISA's vulnerabilities catalogue

Security Magazine - 14 March 2025 13:00

CISA has announced five known exploited vulnerabilities now in its catalogue, three of which are Ivanti Endpoint Manager flaws.

Recent Fortinet Vulnerabilities Exploited in 'SuperBlack' Ransomware Attacks

SecurityWeek - 14 March 2025 11:05

The newly discovered SuperBlack ransomware has been exploiting two vulnerabilities in Fortinet firewalls.

Threat actors and malware

Malicious Adobe, DocuSign OAuth apps target Microsoft 365 accounts

BleepingComputer - 16 March 2025 11:19

Cybercriminals are promoting malicious Microsoft OAuth apps that masquerade as Adobe and DocuSign apps to deliver malware and steal Microsoft 365 accounts credentials. [...]

New Akira ransomware decryptor cracks encryptions keys using GPUs

BleepingComputer - 15 March 2025 11:16

Security researcher Yohanes Nugroho has released a decryptor for the Linux variant of Akira ransomware, which utilizes GPU power to retrieve the decryption key and unlock files for free. [...]

Ransomware gang creates tool to automate VPN brute-force attacks

BleepingComputer - 14 March 2025 13:55

The Black Basta ransomware operation created an automated brute-forcing framework dubbed 'BRUTED' to breach edge networking devices like firewalls and VPNs. […]

Denmark warns of increased state-sponsored campaigns targeting the European telcos

Security Affairs - 17 March 2025 00:43

Denmark 's cybersecurity agency warns of increased state-sponsored campaigns targeting the European telecom companies Denmark raised the cyber espionage threat level for its telecom sector from medium to high due to rising threats across Europe. The Danish Social Security Agency published a new threat assessment for the cyber threat to the telecommunications sector that highlights […]

SuperBlack Ransomware operators exploit Fortinet Firewall flaws in recent attacks

Security Affairs - 14 March 2025 13:02

Operators behind the SuperBlack ransomware exploited two vulnerabilities in Fortinet firewalls for recent attacks. Between January and March, researchers at Forescout Research – Vedere Labs observed a threat actors exploiting two Fortinet vulnerabilities to deploy the SuperBlack ransomware. The experts attribute the attacks to a threat actor named "Mora_001" which using Russian-language artifacts and exhibiting […]

OBSCURE#BAT Malware Uses Fake CAPTCHA Pages to Deploy Rootkit r77 and Evade Detection

The Hacker News - 14 March 2025 12:07

A new malware campaign has been observed leveraging social engineering tactics to deliver an open-source rootkit called r77.The activity, condemned OBSCURE#BAT by Securonix, enables threat actors to establish persistence and evade detection on compromised systems. It's currently not known who is behind the campaign.The rootkit "has the ability to cloak or mask any file, registry key or task

UK related

Apple's alleged UK encryption battle sparks political and privacy backlash

The Register - 14 March 2025 14:09

National security defense being used to keep appeal behind closed doors US politicians and privacy campaigners are calling for the private hearing between Apple and the UK government regarding its alleged encryption-busting order to be aired in public....