Scottish Cyber Coordination Centre

Daily Threat Bulletin

20 March 2025

Vulnerabilities

IBM scores perfect 10 ... vulnerability in mission-critical OS AIX

The Register - 19 March 2025 19:58

IBM “strongly recommends” customers running its Advanced Interactive eXecutive (AIX) operating system apply patches after disclosing two critical vulnerabilities, one of which has a perfect 10 severity score.

WhatsApp patched zero-click flaw exploited in Paragon spyware attacks

BleepingComputer - 19 March 2025 13:02

WhatsApp has patched a zero-click, zero-day vulnerability used to install Paragon’s Graphite spyware following reports from security researchers at the University of Toronto’s Citizen Lab.

Critical Fortinet Vulnerability Draws Fresh Attention

darkreading - 19 March 2025 22:19

CISA this week added CVE-2025-24472 to its catalog of known exploited vulnerabilities, citing ransomware activity targeting the authentication bypass flaw.

Threat actors and malware

Malware campaign ‘DollyWay’ breached 20,000 WordPress sites

BleepingComputer - 19 March 2025 20:12

A malware operation dubbed ‘DollyWay’ has been underway since 2016, compromising over 20,000 WordPress sites globally to redirect users to malicious sites.

CERT-UA Warns: Dark Crystal RAT Targets Ukrainian Defense via Malicious Signal Messages

The Hacker News - 20 March 2025 12:38

The Computer Emergency Response Team of Ukraine (CERT-UA) is warning of a new campaign that targets the defense sectors with Dark Crystal RAT (aka DCRat). The campaign, detected earlier this month, has been found to target both employees of enterprises of the defense-industrial complex and individual representatives of the Defense Forces of Ukraine.

Scottish Cyber Coordination Centre

Microsoft Warns of New StilachiRAT Malware

SecurityWeek - 19 March 2025 10:59

Microsoft has shared details on StilachiRAT, an evasive and persistent piece of malware that facilitates sensitive data theft.

Sneaky 2FA Joins Tycoon 2FA and EvilProxy in 2025 Phishing Surge

Infosecurity Magazine - 19 March 2025 12:30

Security firm Barracuda said it has detected more than a million phishing-as-a-service (PhaaS) attacks in 2025.

Leaked Black Basta Chats Suggest Russian Officials Aided Leader's Escape from Armenia

The Hacker News - 19 March 2025 20:20

The recently leaked trove of internal chat logs among members of the Black Basta ransomware operation has revealed possible connections between the e-crime gang and Russian authorities.

Chinese Hacking Group MirrorFace Targeting Europe

SecurityWeek - 19 March 2025 13:59

Chinese hacking group MirrorFace has targeted a Central European diplomatic institute with the Anel backdoor and AsyncRAT.