Scottish Cyber Coordination Centre

Daily threat bulletin

26 April 2024

Vulnerabilities

Vulnerabilities Expose Brocade SAN Appliances, Switches to Hacking

SecurityWeek - 25 April 2024 12:53

The Brocade SANnav management application is affected by multiple vulnerabilities, including a publicly available root password.The post Vulnerabilities Expose Brocade SAN Appliances, Switches to Hacking appeared first on SecurityWeek.

Multiple Vulnerabilities in Hitachi Energy RTU500 Series

CISA Advisories -

The following versions of Hitachi's RTU500 series CMU Firmware are affected: RTU500 series CMU Firmware: Version 12.0.1 - 12.0.14RTU500 series CMU Firmware: Version 12.2.1 - 12.2.11RTU500 series CMU Firmware: Version 12.4.1 - 12.4.11RTU500 series CMU Firmware: Version 12.6.1 - 12.6.9RTU500 series CMU Firmware: Version 12.7.1 - 12.7.6RTU500 series CMU Firmware: Version 13.2.1 - 13.2.6RTU500 series CMU Firmware: Version 13.4.1 - 13.4.4RTU500 series CMU Firmware: Version 13.5.1 - 13.5.33.2.

Cisco Releases Security Updates Addressing ArcaneDoor, Vulnerabilities in Cisco Firewall Platforms

CISA Advisories -

Today, Cisco released security updates to address ArcaneDoor'S exploitation of Cisco Adaptive Security Appliances (ASA) devices and Cisco Firepower Threat Defense (FTD) software. A cyber threat actor could exploit vulnerabilities (CVE-2024-20353, CVE-2024-20359, CVE-2024-20358) to take control of an affected system. Cisco has reported active exploitation of CVE 2024-20353 and CVE-2024-20359 and CISA has added these vulnerabilities to its Known Exploited Vulnerabilities Catalog.

WP Automatic WordPress plugin hit by millions of SQL injection attacks

BleepingComputer - 25 April 2024 11:27

Hackers have started to target a critical severity vulnerability in the WP Automatic plugin for WordPress to create user accounts with administrative privileges and to plant backdoors for long-term access. [...]

Threat actors and malware

Researchers sinkhole PlugX malware server with 2.5 million unique IPs

BleepingComputer - 25 April 2024 16:20

Researchers have sinkholed a command and control server for a variant of the PlugX malware and observed in six months more than 2.5 million connections from unique IP addresses. [...]

North Korea's Lazarus Group Deploys New Kaolin RAT via Fake Job Lures

The Hacker News - 25 April 2024 23:17

The North Korea-linked threat actor known as Lazarus Group employed its time-tested fabricated job lures to deliver a new remote access trojan called Kaolin RAT as part of attacks targeting specific individuals in the Asia region in summer 2023.

Autodesk Drive Abused in Phishing Attacks

SecurityWeek - 25 April 2024 13:25

A new phishing campaign abuses compromised email accounts and targets corporate users with PDF files hosted on Autodesk Drive. The post Autodesk Drive Abused in Phishing Attacksappeared first on SecurityWeek.

DragonForce Ransomware Group Uses LockBit's Leaked Builder

Infosecurity Magazine - 25 April 2024 12:00

Cyber threat intelligence provider Cyble found that DragonForce was using a ransomware binary based on LockBit Black's builder