Scottish Cyber Coordination Centre

Daily threat bulletin

10 May 2024

Vulnerabilities

Citrix warns admins to manually mitigate PuTTY SSH client bug

BleepingComputer - 09 May 2024 16:27

Citrix notified customers this week to manually mitigate a PuTTY SSH client vulnerability that could allow attackers to steal a XenCenter admin's private SSH key. [...]

Mirai botnet also spreads through the exploitation of Ivanti Connect Secure bugs

Security Affairs - 09 May 2024 14:41

Threat actors exploit recently disclosed Ivanti Connect Secure (ICS) vulnerabilities to deploy the Mirai botnet. Researchers from Juniper Threat Labs reported that threat actors are exploiting recently disclosed Ivanti Connect Secure (ICS) vulnerabilities CVE-2023-46805 and CVE-2024-21887 to drop the payload of the Mirai botnet. In early January, the software firm reported that threat actors are exploiting two [...]

Critical F5 Central Manager Vulnerabilities Allow Enable Full Device Takeover

The Hacker News - 09 May 2024 12:41

Two security vulnerabilities have been discovered in F5 Next Central Manager that could be exploited by a threat actor to seize control of the devices and create hidden rogue administrator accounts for persistence.The remotely exploitable flaws "can give attackers full administrative control of the device, and subsequently allow attackers to create accounts on any F5 assets managed by the Next

New 'LLMjacking' Attack Exploits Stolen Cloud Credentials

Infosecurity Magazine - 09 May 2024 17:00

Sysdig said the attackers gained access to these credentials from a vulnerable version of Laravel

New TunnelVision Attack Allows Hijacking of VPN Traffic via DHCP Manipulation

The Hacker News - 10 May 2024 00:25

Researchers have detailed a Virtual Private Network (VPN) bypass technique dubbed TunnelVision that allows threat actors to snoop on victim's network traffic by just being on the same local network.The "decloaking" method has been assigned the CVE identifier CVE-2024-3661 (CVSS score: 7.6). It impacts all operating systems that implement a DHCP client and has

Threat actors and malware

Scottish Cyber Coordination Centre

Zscaler Investigates Hacking Claims After Data Offered for Sale

SecurityWeek - 09 May 2024 08:34

Zscaler says its customer, production and corporate environments are not impacted after a notorious hacker offers to sell access.The post Zscaler Investigates Hacking Claims After Data Offered for Sale appeared first on SecurityWeek.

Monday.com removes “Share Update” feature abused for phishing attacks

BleepingComputer - 09 May 2024 19:17

Project management platform Monday.com has removed its “Share Update” feature after threat actors abused it in phishing attacks. [...]

Dell warns of data breach, 49 million customers allegedly affected

BleepingComputer - 09 May 2024 12:21

Dell is warning customers of a data breach after a threat actor claimed to have stolen information for approximately 49 million customers. [...]

Kremlin-Backed APT28 Targets Polish Institutions in Large-Scale Malware Campaign

The Hacker News - 09 May 2024 21:50

Polish government institutions have been targeted as part of a large-scale malware campaign orchestrated by a Russia-linked nation-state actor called APT28.”The campaign sent emails with content intended to arouse the recipient’s interest and persuade him to click on the link,” the computer emergency response team, CERT Polska, said in a Wednesday bulletin.Clicking on the link

DocGo patient health data stolen in cyberattack

Malwarebytes - 09 May 2024 11:46

Medical health care provider DocGo has disclosed a cyberincident where an attacker gained access to protected health information.

AI-Powered Russian Network Pushes Fake Political News

Infosecurity Magazine - 09 May 2024 12:00

Researchers discover large-scale Russian influence operation using GenAI to influence voters