Scottish Cyber Coordination Centre

Daily threat bulletin

17 April 2024

Vulnerabilities

Ivanti warns of critical flaws in its Avalanche MDM solution

BleepingComputer - 16 April 2024 16:52

Ivanti has released security updates to fix 27 vulnerabilities in its Avalanche mobile device management (MDM) solution, two of them critical heap overflows that can be exploited for remote command execution. [...]

PuTTY SSH Client flaw allows of private keys recovery

Security Affairs - 16 April 2024 19:58

The PuTTY Secure Shell (SSH) and Telnet client are impacted by a critical vulnerability that could be exploited to recover private keys. PuTTY tools from 0.68 to 0.80 inclusive are affected by a critical vulnerability, tracked as CVE-2024-31497, that resides in the code that generates signatures from ECDSA private keys which use the NIST P521 curve. [...]

Delinea Scrambles to Patch Critical Flaw After Failed Responsible Disclosure Attempt

SecurityWeek - 16 April 2024 10:50

PAM company Delinea over the weekend rushed to patch a critical authentication bypass vulnerability after it apparently ignored the researcher who found the flaw.The post Delinea Scrambles to Patch Critical Flaw After Failed Responsible Disclosure Attempt appeared first on SecurityWeek.

LeakyCLI Flaw Exposes AWS and Google Cloud Credentials

Infosecurity Magazine - 16 April 2024 14:15

Orca Security said the issue mirrors a previously identified vulnerability in Azure CLI

Microsoft Issues Patches for 24 New Secure Boot Vulnerabilities

Security Boulevard - 16 April 2024 17:00

Scottish Cyber Coordination Centre

Threat actors and malware

[Cisco warns of large-scale brute-force attacks against VPN and SSH services]

Security Affairs - 17 April 2024 06:02

Cisco Talos warns of large-scale brute-force attacks against a variety of targets, including VPN services, web application authentication interfaces and SSH services. Cisco Talos researchers warn of large-scale credential brute-force attacks targeting multiple targets, including Virtual Private Network (VPN) services, web application authentication interfaces and SSH services since at least March 18, 2024.

[Ransomware group Dark Angels claims the theft of 1TB of data from chipmaker Nexperia]

Security Affairs - 16 April 2024 08:08

The Dark Angels (Dunghill) ransomware group claims the hack of the chipmaker Nexperia and the theft of 1 TB of data from the company. The Dark Angels (Dunghill) ransomware group claims responsibility for hacking chipmaker Nexperia and stealing 1 TB of the company';s data. Nexperia is a semiconductor manufacturer headquartered in Nijmegen, the Netherlands.

[TA558 Hackers Weaponize Images for Wide-Scale Malware Attacks]

The Hacker News - 16 April 2024 20:09

The threat actor tracked as TA558 has been observed leveraging steganography as an obfuscation technique to deliver a wide range of malware such as Agent Tesla, FormBook, Remcos RAT, LokiBot, GuLoader, Snake Keylogger, and XWorm, among others.

[LockBit 3.0 Variant Generates Custom, Self-Propagating Malware]

darkreading - 16 April 2024 14:41

Kaspersky researchers discovered the new variant after responding to a critical incident targeting an organization in West Africa.

[Ransomware Group Starts Leaking Data Allegedly Stolen From Change Healthcare]

SecurityWeek - 16 April 2024 12:29

The RansomHub group has started leaking information allegedly stolen from Change Healthcare in February 2024.The post Ransomware Group Starts Leaking Data Allegedly Stolen From Change Healthcare appeared first on SecurityWeek.