Scottish
Cyber
Coordination
Centre

Daily threat bulletin

18 July 2024

Vulnerabilities

A critical flaw in Cisco SSM On-Prem allows attackers to change any user's password

Security Affairs - 18 July 2024 00:03

A vulnerability in Cisco Smart Software Manager On-Prem (Cisco SSM On-Prem) license servers allows threat actors to change any user's password. Cisco has addressed a critical vulnerability, tracked as CVE-2024-20419 (CVSS score of 10.0), in Cisco Smart Software Manager On-Prem (Cisco SSM On-Prem) license servers that allows attackers to change any user's password.

Void Banshee exploits CVE-2024-38112 zero-day to spread malware

Security Affairs - 17 July 2024 15:16

Void Banshee APT group exploited the Windows zero-day CVE-2024-38112 to execute code via the disabled Internet Explorer. An APT group tracked as Void Banshee was spotted exploiting the Windows zero-day CVE-2024-38112 (CVSS score of 7.5) to execute code through the disabled Internet Explorer.

Chrome 126 Updates Patch High-Severity Vulnerabilities

SecurityWeek - 17 July 2024 10:20

Chrome 126 security updates released this week resolve high-severity vulnerabilities reported by external researchers.

Oracle Patches 240 Vulnerabilities With July 2024 CPU

SecurityWeek - 17 July 2024 09:47

Oracle releases 386 new security patches to resolve roughly 240 unique CVEs as part of its July 2024 Critical Patch Update.

Threat actors and malware

Notorious FIN7 hackers sell EDR killer to other threat actors

BleepingComputer - 17 July 2024 18:11

The notorious FIN7 hacking group has been spotted selling its custom "AvNeutralizer" tool, used to evade detection by killing enterprise endpoint protection software on corporate networks.

North Korean Hackers Update BeaverTail Malware to Target MacOS Users

The Hacker News - 17 July 2024 22:57

Cybersecurity researchers have discovered an updated variant of a known stealer malware that attackers affiliated with the Democratic People's Republic of Korea (DPRK) have delivered as part of prior cyber espionage campaigns targeting job seekers.The artifact in question is an Apple macOS disk image (DMG) file named "MiroTalk.dmg" that mimics the legitimate video call service of the same name, but, in reality, serves as a conduit to deliver a native version of BeaverTail.

China-linked APT17 Targets Italian Companies with 9002 RAT Malware

The Hacker News - 17 July 2024 15:17

A China-linked threat actor called APT17 has been observed targeting Italian companies and government entities using a variant of a known malware referred to as 9002 RAT. The two targeted attacks took place on June 24 and July 2, 2024, Italian cybersecurity company TG Soft said in an analysis published last week.

'BadPack' APK Files Make Android Malware Hard to Detect

darkreading - 17 July 2024 16:27

"BadPack," a set of maliciously packaged APK files that make it difficult for researchers to analyze and detect malware within Android applications, has come to light.