Scottish Cyber Coordination Centre

Daily threat bulletin

25 July 2024

Vulnerabilities

Docker fixes critical 5-year old authentication bypass flaw

BleepingComputer - 24 July 2024 16:00

Docker has issued security updates to address a critical vulnerability impacting certain versions of Docker Engine that could allow an attacker to bypass authorization plugins (AuthZ) under certain circumstances.

Microsoft fixes bug behind Windows 10 Connected Cache delivery issues

BleepingComputer - 24 July 2024 15:05

Microsoft has fixed a known Windows 10 update issue that broke Microsoft Connected Cache (MCC) node discovery on enterprise networks.

Telegram App Flaw Exploited to Spread Malware Hidden in Videos

The Hacker News - 24 July 2024 18:29

A zero-day security flaw in Telegram's mobile app for Android called EvilVideo made it possible for attackers to malicious files disguised as harmless-looking videos.The exploit appeared for sale for an unknown price in an underground forum on June 6, 2024.

CrowdStrike Blames Crash on Buggy Security Content Update

darkreading - 24 July 2024 15:26

CrowdStrike vows to provide customers with greater control over the delivery of future content updates by allowing granular selection of when and where these updates are deployed.

Chrome 127 Patches 24 Vulnerabilities

SecurityWeek - 24 July 2024 12:33

Chrome 127 was promoted to the stable channel with patches for 24 vulnerabilities, including 16 reported externally.

Threat actors and malware

Chinese hackers deploy new Macma macOS backdoor version

BleepingComputer - 23 July 2024 20:33

The Chinese hacking group tracked as 'Evasive Panda' was spotted using new versions of the Macma backdoor and the Nightdoor Windows malware. [...]

Scottish Cyber Coordination Centre

Hackers abused swap files in e-skimming attacks on Magento sites

Security Affairs - 23 July 2024 18:28

Threat actors abused swap files in compromised Magento websites to hide credit card skimmer and harvest payment information. Security researchers from Sucuri observed threat actors using swap files in compromised Magento websites to conceal a persistent software skimmer and harvest payment information. The attackers used this tactic to maintain persistence and allowing the malware to [...]

Chinese Espionage Group Upgrades Malware Arsenal to Target All Major OS

Infosecurity Magazine - 23 July 2024 16:00

Symantec said Chinese espionage group Daggerfly has updated its malware toolkit as it looks to target Windows, Linux, macOS and Android operating systems

BreachForums v1 hacking forum data leak exposes members' info

BleepingComputer - 23 July 2024 16:24

The private member information of the BreachForums v1 hacking forum from 2022 has been leaked online, allowing threat actors and researchers to gain insight into its users. [...]

New ICS Malware 'FrostyGoop' Targeting Critical Infrastructure

The Hacker News - 23 July 2024 17:24

Cybersecurity researchers have discovered what they say is the ninth Industrial Control Systems (ICS)-focused malware that has been used in a disruptive cyber attack targeting an energy company in the Ukrainian city of Lviv earlier this January.Industrial cybersecurity firm Dragos has dubbed the malware FrostyGoop, describing it as the first malware strain to directly use Modbus TCP