Scottish Cyber Coordination Centre

Daily threat bulletin

4 July 2024

Vulnerabilities

CVE of the month, the supply chain attack hidden for 10 years CVE-2024-38368

Security Boulevard - 03 July 2024 19:32

For over a decade, a massive vulnerability that could have unleashed a huge supply chain attack lay dormant. Luckily the good guys found it first or so it seems. This month we are taking a look at CVE-2024-38368.

Microsoft Uncovers Major Flaws in Rockwell PanelView Plus

Infosecurity Magazine - 03 July 2024 16:30

Microsoft's cybersecurity team has uncovered two significant vulnerabilities in Rockwell Automation's PanelView Plus, a type of human-machine interface (HMI) widely used in industrial settings. These vulnerabilities, identified as CVE-2023-2071 and CVE-2023-29464, can be exploited remotely by unauthenticated attackers to perform remote code execution (RCE) and denial-of-service (DoS) respectively.

CISA Adds One Known Exploited Vulnerability to Catalog

CISA Advisories -

CISA has added one new vulnerability to its Known Exploited Vulnerabilities Catalog, based on evidence of active exploitation. CVE-2024-20399 Cisco NX-OS Command Injection Vulnerability. These types of vulnerabilities are frequent attack vectors for malicious cyber actors and pose significant risks to the federal enterprise.

Threat actors and malware

OVHcloud blames record-breaking DDoS attack on MikroTik botnet

BleepingComputer - 03 July 2024 15:07

OVHcloud, a global cloud services provider and one of the largest of its kind in Europe, says it mitigated a record-breaking distributed denial of service (DDoS) attack earlier this year that reached an unprecedented packet rate of 840 million packets per second (Mpps).

Hackers abused API to verify millions of Authy MFA phone numbers

BleepingComputer - 03 July 2024 13:43

Twilio has confirmed that an unsecured API endpoint allowed threat actors to verify the phone numbers of millions of Authy multi-factor authentication users, potentially making them vulnerable to SMS phishing and SIM swapping attacks.

Scottish Cyber Coordination Centre

Microsoft MSHTML Flaw Exploited to Deliver MerkSpy Spyware Tool

The Hacker News - 03 July 2024 16:23

Unknown threat actors have been observed exploiting a now-patched security flaw in Microsoft MSHTML to deliver a surveillance tool called MerkSpy as part of a campaign primarily targeting users in Canada, India, Poland, and the U.S."MerkSpy is designed to clandestinely monitor user activities, capture sensitive information, and establish persistence on compromised systems.

Operation Morpheus took down 593 Cobalt Strike servers used by threat actors

Security Affairs - 03 July 2024 19:22

An international law enforcement operation code-named Operation Morpheus led to the takedown of 593 Cobalt Strike servers used by crooks. An international law enforcement operation, code-named Operation Morpheus, aimed at combatting the criminal abuse of an older, unlicensed version of the Cobalt Strike red teaming tool. The Cobalt Strike platform was developed for Adversary Simulations.

FakeBat Loader Malware Spreads Widely Through Drive-by Download Attacks

The Hacker News - 03 July 2024 13:35

The loader-as-a-service (LaaS) known as FakeBat has become one of the most widespread loader malware families distributed using the drive-by download technique this year, findings from Sekoia reveal. "FakeBat primarily aims to download and execute the next-stage payload, such as IcedID, Lumma, RedLine, SmokeLoader, SectopRAT, and Ursnif," the company said in a Tuesday analysis.

Ransomware Eruption: Novel Locker Malware Flows From ‘Volcano Demon’

darkreading - 03 July 2024 17:41

Attackers clear logs before exploitation and use 'no caller' numbers to negotiate ransoms, complicating detection and forensics efforts.