Scottish Cyber Coordination Centre

Daily threat bulletin

5 July 2024

Vulnerabilities

Splunk fixed tens of flaws in Splunk Enterprise and Cloud Platform

Security Affairs - 04 July 2024 09:03

Technology company Splunk released security updates to address 16 vulnerabilities in Splunk Enterprise and Cloud Platform. The company addressed 16 vulnerabilities in Splunk Enterprise and Cloud Platform, including four high-severity flaws.

Microsoft Uncovers Critical Flaws in Rockwell Automation PanelView Plus

The Hacker News - 04 July 2024 15:40

Microsoft has revealed two security flaws in Rockwell Automation PanelView Plus that could be weaponized by remote, unauthenticated attackers to execute arbitrary code and trigger a denial-of-service (DoS) condition. The remote code execution vulnerability in PanelView Plus involves two custom classes that can be abused to upload and load a malicious DLL into the device.

Threat actors and malware

New Golang-Based Zergeca Botnet Capable of Powerful DDoS Attacks

The Hacker News - 05 July 2024 10:22

Cybersecurity researchers have uncovered a new botnet called Zergeca that's capable of conducting distributed denial-of-service (DDoS) attacks. Written in Golang, the botnet is so named for its reference to a string named "ootheca" present in the command-and-control (C2) servers ("ootheca[.]pw" and "ootheca[.]top").

Polyfill Attack Impacts Over 380,000 Hosts, Including Major Companies

The Hacker News - 05 July 2024 10:48

The supply chain attack targeting widely-used Polyfill[.]io JavaScript library is wider in scope than previously thought, with new findings from Censys showing that over 380,000 hosts are embedding a polyfill script linking to the malicious domain as of July 2, 2024.This includes references to "https://cdn.polyfill[.]io" or "https://cdn.polyfill[.]com" in their HTTP responses, the attack

UK incidents

UK’s NCA Leads Major Cobalt Strike Takedown

Infosecurity Magazine - 04 July 2024 09:30

Global law enforcers have share intelligence leading to the takedown of hundreds of IP addresses hosting Cobalt Strike. The UK's National Crime Agency (NCA) has revealed details of an ambitious operation to disrupt the cybercrime supply chain by targeting IP addresses hosting the Cobalt Strike tool.