Scottish Cyber Coordination Centre

Daily threat bulletin

4 November 2024

Vulnerabilities

Microsoft SharePoint RCE bug exploited to breach corporate network

BleepingComputer - 02 November 2024 12:19

A recently disclosed Microsoft SharePoint remote code execution (RCE) vulnerability tracked as CVE-2024-38094 is being exploited to gain initial access to corporate networks. [...]

Synology hurries out patches for zero-days exploited at Pwn2Own

BleepingComputer - 01 November 2024 13:38

Synology, a Taiwanese network-attached storage (NAS) appliance maker, patched two critical zero-days exploited during last week's Pwn2Own hacking competition within days. [...]

PTZOptics cameras zero-days actively exploited in the wild

Security Affairs - 02 November 2024 08:16

Hackers are exploiting two zero-day vulnerabilities, tracked as CVE-2024-8956 and CVE-2024-8957, in PTZOptics cameras. Threat actors are attempting to exploit two zero-day vulnerabilities, tracked as CVE-2024-8956 and CVE-2024-8957, in PTZOptics pan-tilt-zoom (PTZ) live streaming cameras, GretNoise researchers warn. GreyNoise discovered the two flaws while investigating the use of an exploit detected by its LLM-powered threat-hunting tool Sift.

Critical Auth Bugs Expose Smart Factory Gear to Cyberattack

darkreading - 01 November 2024 18:15

Factory automation software from Mitsubishi Electric and Rockwell Automation could be subject to remote code execution (RCE), denial-of-service (DoS), and more.

GreyNoise: AI's Central Role in Detecting Security Flaws in IoT Devices

Security Boulevard - 01 November 2024 21:45

GreyNoise Intelligence researchers said proprietary internal AI-based tools allowed them to detect and identify two vulnerabilities in IoT live-stream cameras that traditional cybersecurity technologies would not have been able to discover.

Threat actors and malware

Chinese threat actors use Quad7 botnet in password-spray attacks

Security Affairs - 03 November 2024 11:09

Scottish Cyber Coordination Centre

Microsoft warns Chinese threat actors are using the Quad7 botnet to carry out password-spray attacks and steal credentials.

New Phishing Kit Xiū gǒu Targets Users Across Five Countries With 2,000 Fake Sites

The Hacker News - 01 November 2024 10:20

Cybersecurity researchers have disclosed a new phishing kit that has been put to use in campaigns targeting Australia, Japan, Spain, the U.K., and the U.S. since at least September 2024.

NCSC Details 'Pygmy Goat' Backdoor Planted on Hacked Sophos Firewall Devices

SecurityWeek - 01 November 2024 15:41

A stealthy network backdoor found on hacked Sophos XG firewall devices is programmed to work on a broader range of Linux-based devices.

Foreign Threat Actor Conducting Large-Scale Spear-Phishing Campaign with RDP Attachments

CISA Advisories -

CISA has received multiple reports of a large-scale spear-phishing campaign targeting organizations in several sectors, including government and information technology (IT). The foreign threat actor, often posing as a trusted entity, is sending spear-phishing emails containing malicious remote desktop protocol (RDP) files to targeted organizations to connect to and access files stored on the target's network.

UK related

UK councils bat away DDoS barrage from pro-Russia keyboard warriors

The Register - 01 November 2024 11:58

Local authority websites downed in response to renewed support for Ukraine Multiple UK councils had their websites either knocked offline or were inaccessible to residents this week after pro-Russia cyber nuisances added them to a daily target list....