Scottish Cyber Coordination Centre

Daily threat bulletin

1 November 2024

Vulnerabilities

Hackers target critical zero-day vulnerability in PTZ cameras

BleepingComputer - 31 October 2024 15:23

Hackers are attempting to exploit two zero-day vulnerabilities in PTZOptics pan-tilt-zoom (PTZ) live streaming cameras used in industrial, healthcare, business conferences, government, and courtroom settings. [...]

Windows 11 Task Manager bug shows wrong number of running processes

BleepingComputer - 31 October 2024 13:45

Microsoft is investigating a new Windows 11 issue that causes the Task Manager to say there are zero running apps and background processes. [...]

Microsoft fixes Windows 10 bug causing apps to stop working

BleepingComputer - 31 October 2024 11:40

Microsoft has fixed a known issue that prevents some apps launched from non-admin accounts from starting on Windows 10 22H2 systems after installing the September preview cumulative update. [...]

Yahoo Discloses NetIQ iManager Flaws Allowing Remote Code Execution

SecurityWeek - 31 October 2024 13:50

Yahoo researchers found nearly a dozen vulnerabilities in OpenText's NetIQ iManager and some could have been chained for unauthenticated RCE.

Threat actors and malware

Microsoft: Chinese hackers use Quad7 botnet to steal credentials

BleepingComputer - 31 October 2024 17:03

Microsoft warns that Chinese threat actors use the Quad7 botnet, compromised of hacked SOHO routers, to steal credentials in password-spray attacks. [...]

CyberPanel Vulnerabilities Exploited in Ransomware Attacks Shortly After Disclosure

SecurityWeek - 31 October 2024 11:06

CyberPanel vulnerabilities have been exploited to compromise thousands of instances as part of ransomware attacks.

Scottish Cyber Coordination Centre

Misconfigured Git Configurations Targeted in Emeraldwhale Attack

Infosecurity Magazine - 31 October 2024 17:30

Emeraldwhale breach allowed access to over 10,000 repositories and resulted in the theft of more than 15,000 cloud service credentials

Sophos reveals 5-year battle with Chinese hackers attacking network devices

BleepingComputer - 31 October 2024 19:16

Sophos disclosed today a series of reports dubbed “Pacific Rim” that detail how the cybersecurity company has been sparring with Chinese threat actors for over 5 years as they increasingly targeted networking devices worldwide, including those from Sophos. [...]