Scottish Cyber Coordination Centre

# Daily threat bulletin

7 November 2024

## Vulnerabilities

### Synology fixed critical flaw impacting millions of DiskStation and BeePhotos NAS devices

Security Affairs - 06 November 2024 10:09

Synology addressed a critical vulnerability in DiskStation and BeePhotos NAS devices that could lead to remote code execution. Taiwanese vendor Synology has addressed a critical security vulnerability, tracked as CVE-2024-10443, that impacts DiskStation and BeePhotos. An attacker can exploit the flaw without any user interaction and successful exploitation of this flaw could lead to remote [...]

### Cisco Releases Patch for Critical URWB Vulnerability in Industrial Wireless Systems

The Hacker News - 07 November 2024 13:43

Cisco has released security updates to address a maximum severity security flaw impacting Ultra-Reliable Wireless Backhaul (URWB) Access Points that could permit unauthenticated, remote attackers to run commands with elevated privileges. Tracked as CVE-2024-20418 (CVS score: 10.0), the vulnerability has been described as stemming from a lack of input validation to the web-based management.

### Update your Android: Google patches two zero-day vulnerabilities

Malwarebytes - 06 November 2024 13:46

Google has released patches for two zero-days and a lot of other high level vulnerabilities.

## Threat actors and malware

### Hackers increasingly use Winos4.0 post-exploitation kit in attacks

BleepingComputer - 06 November 2024 17:25

Hackers are increasingly targeting Windows users with the malicious Winos4.0 framework, distributed via seemingly benign game-related apps. [...]

### New SteelFox malware hijacks Windows PCs using vulnerable driver

BleepingComputer - 06 November 2024 13:53

A new malicious package called 'SteelFox' mines for cryptocurrency and steals credit card data by using the "bring your own vulnerable driver" technique to get SYSTEM privileges on Windows machines. [...]

### Critical bug in Cisco UWRB access points allows attackers to run commands as root

Scottish Cyber Coordination Centre

Security Affairs - 07 November 2024 07:17

Cisco fixed a critical flaw in URWB access points, allowing attackers to run root commands, compromising industrial wireless automation security. Cisco has addressed a critical vulnerability, tracked as CVE-2024-20418, that could be exploited by unauthenticated, remote attackers to run commands with root privileges on vulnerable Ultra-Reliable Wireless Backhaul (URWB) access points used for industrial wireless [...]

### VEILDrive Attack Exploits Microsoft Services to Evade Detection and Distribute Malware

The Hacker News - 07 November 2024 00:22

An ongoing threat campaign dubbed VEILDrive has been observed taking advantage of legitimate services from Microsoft, including Teams, SharePoint, Quick Assist, and OneDrive, as part of its modus operandi."Leveraging Microsoft SaaS services — including Teams, SharePoint, Quick Assist, and OneDrive — the attacker exploited the trusted infrastructures of previously compromised organizations to

## UK related

### UK orders Chinese owners to relinquish control of Scottish semiconductor business

The Record from Recorded Future News - 06 November 2024 15:38