Scottish Cyber Coordination Centre

# Daily threat bulletin

12 November 2024

## Vulnerabilities

### Security Flaws in Popular ML Toolkits Enable Server Hijacks, Privilege Escalation

The Hacker News - 11 November 2024 16:41

Cybersecurity researchers have uncovered nearly two dozen security flaws spanning 15 different machine learning (ML) related open-source projects.

### HPE Issues Critical Security Patches for Aruba Access Point Vulnerabilities

The Hacker News - 11 November 2024 16:27

Hewlett Packard Enterprise (HPE) has released security updates to address multiple vulnerabilities impacting Aruba Networking Access Point products, including two critical bugs that could result in unauthenticated command execution.

### Veeam Patches High-Severity Vulnerability as Exploitation of Previous Flaw Expands

SecurityWeek - 11 November 2024 13:01

Veeam has released a hotfix for a high-severity authentication bypass vulnerability in Backup Enterprise Manager.

### Many Legacy D-Link NAS Devices Exposed to Remote Attacks via Critical Flaw

SecurityWeek - 11 November 2024 12:02

D-Link warns of a critical-severity command injection vulnerability impacting multiple discontinued NAS models.

### Palo Alto Networks Addresses Remote Code Execution Vulnerability Claims

SecurityWeek - 11 November 2024 10:56

Palo Alto Networks has issued an advisory urging customers to take action in response to claims of an RCE vulnerability in PAN-OS.

## Threat actors and malware

### New Ymir Ransomware Exploits Memory for Stealthy Attacks; Targets Corporate Networks

The Hacker News - 12 November 2024 12:30

Cybersecurity researchers have flagged a new ransomware family called Ymir that was deployed in an attack two days after systems were compromised by a stealer malware called

RustyStealer."Ymir ransomware introduces a unique combination of technical features and tactics that enhance its effectiveness," Russian cybersecurity vendor Kaspersky said.

### Cybercriminals Use Excel Exploit to Spread Fileless Remcos RAT Malware

The Hacker News - 11 November 2024 12:43

Cybersecurity researchers have discovered a new phishing campaign that spreads a new fileless variant of known commercial malware called Remcos RAT. Remcos RAT provides purchases with a wide range of advanced features to remotely control computers belonging to the buyer.

### Chinese threat actor exploits credentials from password spray attacks

Security Magazine - 11 November 2024 13:00

Microsoft observed malicious activity targeting and stealing credentials from Microsoft customers.

### Flexible Structure of Zip Archives Exploited to Hide Malware Undetected

darkreading - 11 November 2024 18:54

Attackers abuse concatenation, a method that involves appending multiple zip archives into a single file, to deliver a variant of the SmokeLoader Trojan hidden in malicious attachments delivered via phishing