Scottish Cyber Coordination Centre

# Daily Threat Bulletin

29 May 2025

## Vulnerabilities

### Over 100,000 WordPress Sites at Risk from Critical CVSS 10.0 Vulnerability in Wishlist Plugin

The Hacker News - 29 May 2025 12:04

Cybersecurity researchers have disclosed a critical unpatched security flaw impacting TI WooCommerce Wishlist plugin for WordPress that could be exploited by unauthenticated attackers to upload arbitrary files.

### Microsoft OneDrive File Picker Flaw Grants Apps Full Cloud Access — Even When Uploading Just One File

The Hacker News - 28 May 2025 20:11

Cybersecurity researchers have discovered a security flaw in Microsoft's OneDrive File Picker that, if successfully exploited, could allow websites to access a user's entire cloud storage content, as opposed to just the files selected for upload via the tool.

### Chrome 137, Firefox 139 Patch High-Severity Vulnerabilities

SecurityWeek - 28 May 2025 12:36

Google and Mozilla released patches for Chrome and FireFox to address a total of 21 vulnerabilities between the two browsers, including three rated high severity.

## Threat actors and malware

### Interlock ransomware gang deploys new NodeSnake RAT on universities

BleepingComputer - 28 May 2025 15:14

The Interlock ransomware gang is deploying a previously undocumented remote access trojan (RAT) named NodeSnake against educational institutes for persistent access to corporate networks.

### APT41 malware abuses Google Calendar for stealthy C2 communication

BleepingComputer - 28 May 2025 19:04

The Chinese APT41 hacking group uses a new malware named 'ToughProgress' that abuses Google Calendar for command-and-control (C2) operations, hiding malicious activity behind a trusted cloud service.

Scottish Cyber Coordination Centre

### DragonForce double-whammy: First hit an MSP, then use RMM software to push ransomware

The Register - 28 May 2025 07:45

DragonForce ransomware infected a managed service provider, and its customers, after attackers exploited security flaws in remote monitoring and management tool SimpleHelp.

### Crooks use a fake antivirus site to spread Venom RAT and a mix of malware

Security Affairs - 28 May 2025 10:02

Researchers warn of a malicious campaign using a fake website ("bitdefender-download[.]com") spoofing Bitdefender's Antivirus for Windows download page to trick visitors into downloading a remote access trojan called Venom RAT.

### Botnet hacks 9,000+ ASUS routers to add persistent SSH backdoor

BleepingComputer - 28 May 2025 13:44

Over 9,000 ASUS routers are compromised by a novel botnet dubbed "AyySSHush" that was also observed targeting SOHO routers from Cisco, D-Link, and Linksys.

### New Russian State Hacking Group Hits Europe and North America

Infosecurity Magazine - 28 May 2025 09:15

A newly-discovered Russian group, Void Blizzard, has successfully compromised organisations in critical industries, Microsoft warned

## UK incidents

### Ivanti Vulnerability Exploit Could Expose UK NHS Data

Infosecurity Magazine - 28 May 2025 16:15

Two healthcare organisations in the UK are said to be among the victims of a malicious campaign involving the exploitation of a vulnerability linked to cybersecurity hardware provider Ivanti. Both trusts could see highly sensitive patient records exposed.