Scottish Cyber Coordination Centre

# Daily Threat Bulletin

9 October 2025

## Vulnerabilities

### Hackers exploit auth bypass in Service Finder WordPress theme

BleepingComputer - 08 October 2025 12:57

Threat actors are actively exploiting a critical vulnerability in the Service Finder WordPress theme that allows them to bypass authentication and log in as administrators.

### Severe Figma MCP Vulnerability Lets Hackers Execute Code Remotely — Patch Now

The Hacker News - 08 October 2025 17:28

Cybersecurity researchers have disclosed details of a now-patched vulnerability in the popular figma-developer-mcp Model Context Protocol (MCP) server that could allow attackers to achieve code execution.

### Exploitation of Oracle EBS Zero-Day Started 2 Months Before Patching

SecurityWeek - 08 October 2025 08:45

Hundreds of internet-exposed Oracle E-Business Suite instances may still be vulnerable to attacks.

## Threat actors and malware

### New FileFix attack uses cache smuggling to evade security software

BleepingComputer - 08 October 2025 16:49

A new variant of the FileFix social engineering attack uses cache smuggling to secretly download a malicious ZIP archive onto a victim's system and bypassing security software.

### Nezha Tool Used in New Cyber Campaign Targeting Web Applications

Infosecurity Magazine - 08 October 2025 14:00

A cyber campaign using Nezha has been identified, targeting vulnerable web apps with PHP web shells and Ghost RAT.

Scottish Cyber Coordination Centre

### LockBit, Qilin, and DragonForce Join Forces to Dominate the Ransomware Ecosystem

The Hacker News - 08 October 2025 18:34

Three prominent ransomware groups DragonForce, LockBit, and Qilin have announced a new strategic ransomware alliance, once underscoring continued shifts in the cyber threat landscape.The coalition is seen as an attempt on the part of the financially motivated threat actors to conduct more effective ransomware attacks.

### Red Hat Hackers Team Up With Scattered Lapsus$ Hunters

darkreading - 08 October 2025 21:40

Crimson Collective, which recently breached the GitLab instance of Red Hat Consulting, has teamed up with the notorious cybercriminal collective.

### Hackers claim Discord breach exposed data of 5.5 million users

BleepingComputer - 08 October 2025 21:22

Discord says they will not be negotiating with threat actors who claim to have stolen the data of 5.5 million unique users from the company's Zendesk support system instance, including government IDs and partial payment information for some people.

## UK incidents

### London police arrests suspects linked to nursery breach, child doxing

BleepingComputer - 08 October 2025 11:49

The UK Metropolitan Police has arrested two suspects following an investigation into the doxing of children online after a ransomware attack on a chain of London-based nurseries.