



# Daily Threat Bulletin

12 December 2025

## Vulnerabilities

### [Google Patches Mysterious Chrome Zero-Day Exploited in the Wild](#)

SecurityWeek - 11 December 2025 08:43

The Chrome zero-day does not have a CVE and it's unclear who reported it and which browser component it affects.

### [Hackers exploit Gladinet CentreStack cryptographic flaw in RCE attacks](#)

BleepingComputer - 11 December 2025 17:49

Hackers are exploiting a new, undocumented vulnerability in the implementation of the cryptographic algorithm present in Gladinet's CentreStack and Triofox products for secure remote file access and sharing.

### [Critical Gogs zero-day under attack, 700 servers hacked](#)

Security Affairs - 11 December 2025 22:29

Hackers exploited an unpatched Gogs zero-day, allowing remote code execution and compromising around 700 Internet-facing servers. Gogs is a self-hosted Git service, similar to GitHub, GitLab, or Bitbucket, but designed to be lightweight and easy to deploy.

### [CISA Adds One Known Exploited Vulnerability to Catalog](#)

CISA Advisories -

CISA has added one new vulnerability to its Known Exploited Vulnerabilities (KEV) Catalog, based on evidence of active exploitation.

CVE-2025-58360 OSGeo GeoServer Improper Restriction of XML External Entity Reference Vulnerability

### [IBM Patches Over 100 Vulnerabilities](#)

SecurityWeek - 11 December 2025 11:23

Most of the 100 vulnerabilities resolved this week, including critical flaws, were in third-party dependencies.

## Threat actors and malware



Scottish  
Cyber  
Coordination  
Centre

### **[New ConsentFix attack hijacks Microsoft accounts via Azure CLI](#)**

BleepingComputer - 11 December 2025 11:10

A new variation of the ClickFix attack dubbed 'ConsentFix' abuses the Azure CLI OAuth app to hijack Microsoft accounts without the need for a password or to bypass multi-factor authentication (MFA) verifications.

### **[NANOREMOTE Malware Uses Google Drive API for Hidden Control on Windows Systems](#)**

The Hacker News - 11 December 2025 19:46

Cybersecurity researchers have disclosed details of a new fully-featured Windows backdoor called NANOREMOTE that uses the Google Drive API for command-and-control (C2) purposes.

### **[Wide Range of Malware Delivered in React2Shell Attacks](#)**

SecurityWeek - 11 December 2025 13:12

Security firms have seen cryptocurrency miners, Linux backdoors, botnet malware, and various post-exploitation implants in React2Shell attacks.

### **[Malware Discovered in 19 Visual Studio Code Extensions](#)**

Infosecurity Magazine - 11 December 2025 17:00

A new campaign involving 19 malicious Visual Studio Code extensions used a legitimate npm package to embed malware in dependency folders

### **[GOLD SALEM tradecraft for deploying Warlock ransomware](#)**

Threat Research – Sophos News - 11 December 2025 11:00

Analysis of the tradecraft evolution across 6 months and 11 incidents

## **UK incidents**

### **[Users report chaos as Legal Aid Agency stumbles back online after cyberattack](#)**

The Register - 11 December 2025 10:30

Seven months after a landmark cyberattack, the UK's Legal Aid Agency (LAA) says it's returning to pre-breach operations, although law firms are still wrestling with buggy and more laborious systems.

### **[UK fines LastPass £1.2 million for data breach affecting 1.6 million people](#)**

The Record from Recorded Future News - 11 December 2025 15:58

The British subsidiary of password management company LastPass was fined £1.2 million on Thursday by the United Kingdom's privacy regulator for a data breach in 2022.