Scottish Cyber Coordination Centre

# Daily Threat Bulletin

21 April 2026

## Vulnerabilities

### CVE-2023-33538 under attack for a year, but exploitation still unsuccessful

Security Affairs - 20 April 2026 14:44

Hackers have targeted CVE-2023-33538 flaw in old TP-Link routers for a year, but no successful exploitation has been seen so far. Hackers have been trying for over a year to exploit a serious flaw, tracked as CVE-2023-33538 (CVSS score of 8.8), in outdated TP-Link routers, but so far without success.

### AI Model Claude Opus turns bugs into exploits for just $2,283

Security Affairs - 20 April 2026 09:24

Claude Opus created a working Chrome exploit for $2,283, showing that widely available AI models can already find and weaponize vulnerabilities. Claude Opus managed to produce a functional Chrome exploit for just $2,283, raising concerns about how easily AI can be used to find and exploit vulnerabilities.

### Anthropic MCP Design Vulnerability Enables RCE, Threatening AI Supply Chain

The Hacker News - 20 April 2026 17:12

Cybersecurity researchers have discovered a critical “by design” weakness in the Model Context Protocol’s (MCP) architecture that could pave the way for remote code execution and have a cascading effect on the artificial intelligence (AI) supply chain.

### Serial-to-IP Converter Flaws Expose OT and Healthcare Systems to Hacking

SecurityWeek - 20 April 2026 16:42

Forescout researchers discovered 20 new vulnerabilities in Lantronix and Silex products and described theoretical attack scenarios.

### CISA Adds Eight Known Exploited Vulnerabilities to Catalog

CISA Advisories -

CISA has added eight new vulnerabilities to its Known Exploited Vulnerabilities (KEV) Catalog, based on evidence of active exploitation: CVE-2023-27351 PaperCut NG/MF Improper Authentication Vulnerability; CVE-2024-27199 JetBrains TeamCity Relative Path Traversal Vulnerability; CVE-2025-2749 Kentico Xperience Path Traversal Vulnerability; CVE-2025-32975 Quest KACE Systems Management Appliance (SMA) Improper Authentication Vulnerability; CVE-2025-48700 Synacor Zimbra Collaboration Suite (ZCS) Cross-site Scripting Vulnerability; CVE-2026-20122 Cisco Catalyst SD-WAN Manager Incorrect Use of Privileged APIs Vulnerability; CVE-2026-20128 Cisco Catalyst SD-WAN Manager Storing Passwords in a

Scottish Cyber Coordination Centre

Recoverable Format Vulnerability; CVE-2026-20133 Cisco Catalyst SD-WAN Manager Exposure of Sensitive Information to an Unauthorized Actor Vulnerability.

## Threat actors and malware

### The Gentlemen ransomware now uses SystemBC for bot-powered attacks

BleepingComputer - 20 April 2026 17:02

A SystemBC proxy malware botnet of more than 1,570 hosts, believed to be corporate victims, has been discovered following an investigation into a Gentlemen ransomware attack carried out by a gang affiliate. [...]

### Microsoft: Teams increasingly abused in helpdesk impersonation attacks

BleepingComputer - 20 April 2026 12:11

Microsoft is warning of threat actors increasingly abusing external Microsoft Teams collaboration and relying on legitimate tools for access and lateral movement on enterprise networks. [...]

### France's ANTS ID System website hit by cyberattack, possible data breach

Security Affairs - 20 April 2026 21:30

A cyberattack hit France's ANTS website, possibly exposing personal data from users applying for IDs, passports, and driver's licenses. A cyberattack targeted France's ANTS platform, which handles applications for passports, ID cards, residence permits, and driver's licenses.

### WhatsApp Leaks User Metadata to Attackers

darkreading - 20 April 2026 15:33

Strangers can infer limited info about you without knowing or messaging you, which could theoretically aid certain kinds of malicious activity.

### ZionSiphon Malware Targets Water Infrastructure Systems

Infosecurity Magazine - 20 April 2026 17:00

ZionSiphon malware targets OT water systems with sabotage and ICS scanning capabilities

### Formbook Malware Campaign Uses Multiple Obfuscation Techniques to Avoid Detection

Infosecurity Magazine - 20 April 2026 16:01

Formbook attacks use combination of DLL Side-Loading and Obfuscated JavaScript to stay hidden, researchers at WatchGuard have uncovered

## UK related

### Preparing for severe cyber threat: why leaders must act now

Scottish Cyber Coordination Centre

NCSC - 20 April 2026 13:00

A call to action to collectively build UK resilience.

## British Scattered Spider hacker pleads guilty to crypto theft charges

BleepingComputer - 20 April 2026 10:33

A British man, believed to be the leader of the Scattered Spider cybercrime collective, has pleaded guilty in the United States to charges of wire fraud and aggravated identity theft. [...]