Scottish Cyber Coordination Centre

# Daily Threat Bulletin

11 September 2026

## Vulnerabilities

### CC-4849 - Check Point Releases Security Advisory for Critical Vulnerability in Security Gateway

NHS Digital - 10 September 2026 14:59

Severity: Medium Successful exploitation of CVE-2026-85102 could allow an unauthenticated remote attacker to execute arbitrary code on a vulnerable gateway, potentially leading to complete compromise of the affected device Successful exploitation of CVE-2026-85102 could allow an unauthenticated remote attacker to execute arbitrary code on a vulnerable gateway, potentially leading to complete compromise of the affected device Updated: 10 Sep 2026

### New 'BlueMoon' kit exploited Windows and Chrome zero-day flaws

BleepingComputer - 10 September 2026 11:11

Multiple cyber-espionage groups deployed an exploit kit dubbed "BlueMoon" that leveraged zero-day vulnerabilities in Microsoft Windows and Google Chrome. [...]

### CISA Flags Exploited Cisco, Citrix, Fortinet Flaws, Sets Sept. 12 Federal Patch Deadline

The Hacker News - 10 September 2026 17:06

The U.S. Cybersecurity and Infrastructure Security Agency (CISA) on Wednesday added three flaws, each impacting Cisco, Citrix, and Fortinet, to its Known Exploited Vulnerabilities (KEV) catalog, requiring Federal Civilian Executive Branch (FCEB) agencies to apply the patches by September 12, 2026.

### CISA Adds Two Known Exploited Vulnerabilities to Catalog

CISA Advisories -

CISA has added two new vulnerabilities to its Known Exploited Vulnerabilities (KEV) Catalog, based on evidence of active exploitation. CVE-2026-67277 MikroTik RouterOS Missing Authentication for Critical Function Vulnerability, CVE-2026-86060 MikroTik RouterOS Improper Neutralization of Argument Delimiters in a Command Vulnerability.

## Threat actors and malware

### Hackers Use Claude AI Agents to Automate Cyberattacks, Develop 0-Days and Evade Detection

Cyber Security News - 11 September 2026 03:40

Anthropic's Threat Intelligence team has disclosed a sweeping new report detailing how state-sponsored espionage groups, financially motivated cybercriminals, and lone hacktivists

weaponized its Claude AI models to automate entire cyberattack chains, generate zero-day exploits, and dynamically rewrite malware to slip past security defenses.

### AI-powered attack exploited PaperCut flaws to hack 395 organizations

BleepingComputer - 10 September 2026 12:55

A threat actor, likely Russian-speaking, used hundreds of AI agents to develop and launch a global exploitation campaign targeting vulnerable PaperCut NG/MF servers. [...]

### Cisco FMC flaws exploited by ransomware gang, state-sponsored hackers

BleepingComputer - 10 September 2026 12:43

Cisco Talos says two recently patched Secure Firewall Management Center (FMC) vulnerabilities have been exploited by three separate threat clusters linked to ransomware and state-sponsored attacks. [...]

### Anthropic Discloses Fourth AI Hacking Incident Involving Claude Opus 4.6

The Hacker News - 10 September 2026 13:34

Anthropic on Wednesday disclosed a fourth incident in which its artificial intelligence (AI) model broke into real third-party systems, marking the latest in a growing list of cases that have raised concerns about the security risks posed by autonomous AI agents.

### Critical NetScaler Vulnerability Exploited in Attacks

SecurityWeek - 10 September 2026 13:20

Tracked as CVE-2026-19490, the authentication bypass flaw has been exploited in the wild since at least September 3.

## UK related

### UK Council Attack Linked to Mass Exploitation of SonicWall Flaw

Security Affairs - 11 September 2026 08:11

A critical SonicWall flaw was rapidly weaponized, with a UK Council attack linked to a campaign that exposed credentials and enabled Active Directory theft. On July 17, 2026, the Borough Council of King's Lynn and West Norfolk announced it had detected a cyberattack affecting council services. Hunt.io has since published a detailed technical analysis linking [...]