Scottish Cyber Coordination Centre

# Daily Threat Bulletin

8 September 2025

## Vulnerabilities

### Max severity Argo CD API flaw leaks repository credentials

BleepingComputer - 05 September 2025 12:30

An Argo CD vulnerability allows API tokens with even low project-level get permissions to access API endpoints and retrieve all repository credentials associated with the project. [...]

### Critical SAP S/4HANA flaw CVE-2025-42957 under active exploitation

Security Affairs - 05 September 2025 21:08

Experts warn of an actively exploited vulnerability, tracked as CVE-2025-42957 (CVSS score: 9.9), in SAP S/4HANA software. A critical command injection vulnerability, tracked as CVE-2025-42957 (CVSS score of 9.9), in SAP S/4HANA is under active exploitation.

### WhatsApp Flaw Added to CISA's Known Exploited Vulnerabilities Catalog

Security Magazine - 05 September 2025 09:00

CISA has announced the addition of two vulnerabilities to its Known Exploited Vulnerabilities catalog.

### CISA orders federal agencies to patch Sitecore zero-day following hacking reports

The Record from Recorded Future News - 05 September 2025 14:33

### CISA Adds Three Known Exploited Vulnerabilities to Catalog

CISA Advisories -

CISA has added three new vulnerabilities to its Known Exploited Vulnerabilities (KEV) Catalog, based on evidence of active exploitation: CVE-2025-38352 Linux Kernel Time-of-Check Time-of-Use (TOCTOU) Race Condition Vulnerability; CVE-2025-48543 Android Runtime Unspecified Vulnerability; CVE-2025-53690 Sitecore Multiple Products Deserialization of Untrusted Data Vulnerability.

## Threat actors and malware

### VirusTotal finds hidden malware phishing campaign in SVG files

BleepingComputer - 06 September 2025 15:58

VirusTotal has discovered a phishing campaign hidden in SVG files that create convincing portals impersonating Colombia's judicial system that deliver malware. [...]

Scottish Cyber Coordination Centre

### Czech cyber agency NUKIB flags Chinese espionage risks to critical infrastructure

Security Affairs - 08 September 2025 01:05

Czech cybersecurity agency NUKIB warns of Chinese cyber threats to critical infrastructure, citing the cyberespionage group APT31 and risky devices. The Czech Republic's National Cyber and Information Security Agency (NUKIB) warns of growing risks from Chinese-linked technologies in critical sectors like energy, healthcare, transport, and government.

### Noisy Bear Targets Kazakhstan Energy Sector With BarrelFire Phishing Campaign

The Hacker News - 06 September 2025 21:43

A threat actor possibly of Russian origin has been attributed to a new set of attacks targeting the energy sector in Kazakhstan.The activity, codenamed Operation BarrelFire, is tied to a new threat group tracked by Seqrite Labs as Noisy Bear.

### Shell to pay: Crims invade your PC with CastleRAT malware, now in C and Python

The Register - 05 September 2025 20:45

Pro tip, don't install PowerShell commands without approval A team of data thieves has doubled down by developing its CastleRAT malware in both Python and C variants.

### macOS Stealer Campaign Uses "Cracked" App Lures to Bypass Apple Security

Infosecurity Magazine - 05 September 2025 12:30

Trend Micro observed the attackers using terminal-based installation methods for the AMOS malware, luring macOS users into installing cracked versions of apps

## UK related

### Cyberattack forces Jaguar Land Rover to tell staff to stay at home

The Record from Recorded Future News - 05 September 2025 12:42