Scottish Cyber Coordination Centre

# Daily Threat Bulletin

12 September 2025

## Vulnerabilities

### Akira ransomware exploiting critical SonicWall SSLVPN bug again

BleepingComputer - 11 September 2025 13:32

The Akira ransomware gang is actively exploiting CVE-2024-40766, a year-old critical-severity access control vulnerability, to gain unauthorized access to SonicWall devices. [...]

### Cisco Patches High-Severity IOS XR Vulnerabilities

SecurityWeek - 11 September 2025 15:31

High-severity flaws in IOS XR could lead to ISO image verification bypass and denial-of-service conditions.

### 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-2025-5086 Dassault Systèmes DELMIA Apriso Deserialization of Untrusted Data Vulnerability.

## Threat actors and malware

### Apple warns customers targeted in recent spyware attacks

BleepingComputer - 11 September 2025 16:02

Apple warned customers last week that their devices were targeted in a new series of spyware attacks, according to the French national Computer Emergency Response Team (CERT-FR). [...]

### New VMScape attack breaks guest-host isolation on AMD, Intel CPUs

BleepingComputer - 11 September 2025 12:05

A new Spectre-like attack dubbed VMScape allows a malicious virtual machine (VM) to leak cryptographic keys from an unmodified QEMU hypervisor process running on modern AMD or Intel CPUs. [...]

### Senator Wyden Urges FTC to Probe Microsoft for Ransomware-Linked Cybersecurity Negligence

The Hacker News - 11 September 2025 21:21

U.S. Senator Ron Wyden has called on the Federal Trade Commission (FTC) to probe Microsoft and hold it responsible for what he called “gross cybersecurity negligence” that enabled ransomware attacks on U.S. critical infrastructure, including against healthcare networks.

### Fileless Malware Deploys Advanced RAT via Legitimate Tools

Infosecurity Magazine - 11 September 2025 16:45

A sophisticated fileless malware campaign has been observed using legitimate tools to deliver AsyncRAT executed in memory

## UK related

### UK Train Operator LNER Warns Customers of Data Breach

SecurityWeek - 11 September 2025 14:55

LNER said the security incident involved a third-party supplier and resulted in contact information and other data being compromised.

### Cyberattacks against schools driven by a rise in student hackers, ICO warns

The Record from Recorded Future News - 11 September 2025 15:22