Scottish
Cyber
Coordination
Centre

# Daily Threat Bulletin

3 October 2025

## Vulnerabilities

### Microsoft Defender bug triggers erroneous BIOS update alerts

BleepingComputer - 02 October 2025 11:20

Microsoft is working to resolve a bug that causes Defender for Endpoint to incorrectly tag some devices' BIOS (Basic Input/Output System) firmware as outdated, prompting users to update it.

### DrayTek warns of remote code execution bug in Vigor routers

BleepingComputer - 02 October 2025 14:37

Networking hardware maker DrayTek released an advisory to warn about a security vulnerability in several Vigor router models that could allow remote, unauthenticated actors to execute perform arbitrary code.

### CISA Adds Five Known Exploited Vulnerabilities to Catalog

CISA Advisories -

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

CVE-2014-6278 GNU Bash OS Command Injection Vulnerability
CVE-2015-7755 Juniper ScreenOS Improper Authentication Vulnerability
CVE-2017-1000353 Jenkins Remote Code Execution Vulnerability
CVE-2025-4008 Smartbedded Meteobridge Command Injection Vulnerability
CVE-2025-21043 Samsung Mobile Devices Out-of-Bounds Write Vulnerability

## Threat actors and malware

### Android spyware campaigns impersonate Signal and ToTok messengers

BleepingComputer - 02 October 2025 07:53

Two new spyware campaigns that researchers call ProSpy and ToSpy lured Android users with fake upgrades or plugins for the Signal and ToTok messaging apps to steal sensitive data.

### China-linked APT Phantom Taurus uses Net-Star malware in espionage campaigns against key sectors

Security Affairs - 02 October 2025 08:40

China-linked APT Phantom Taurus targets government and telecom orgs with Net-Star malware for espionage, using unique tactics over two years.

### Confucius Hackers Hit Pakistan With New WooperStealer and Anondoor Malware

The Hacker News - 02 October 2025 21:14

The threat actor known as Confucius has been attributed to a new phishing campaign that has targeted Pakistan with malware families like WooperStealer and Anondoor.

### Google warns of Cl0p extortion campaign against Oracle E-Business users

Security Affairs - 03 October 2025 06:21

Mandiant and Google Threat Intelligence Group (GTIG) researchers are tracking a suspected Cl0p ransomware group's activity, where threat actors attempt to extort executives with claims of stealing Oracle E-Business Suite data.

### CERT-UA warns UAC-0245 targets Ukraine with CABINETRAT backdoor

Security Affairs - 02 October 2025 19:01

The Computer Emergency Response Team of Ukraine (CERT-UA) warned of cyberattacks by the group UAC-0245 using the CABINETRAT backdoor. The campaign, seen in September 2025, involved malicious Excel XLL add-ins posing as software tools (e.g. "UBD Request.xll", "recept_ruslana_nekitenko.xll").