Scottish Cyber Coordination Centre

Daily Threat Bulletin

15 September 2025

Vulnerabilities

CISA warns of actively exploited Dassault RCE vulnerability

BleepingComputer - 12 September 2025 13:19

The U.S. Cybersecurity and Infrastructure Security Agency (CISA) is warning of hackers exploiting a critical remote code execution flaw in DELMIA Apriso, a manufacturing operations management (MOM) and execution (MES) solution from French company Dassault Systèmes. [...]

Cisco fixes high-severity IOS XR flaws enabling image bypass and DoS

Security Affairs - 12 September 2025 15:17

Cisco addressed multiple high-severity IOS XR vulnerabilities that can allow ISO image verification bypass and trigger DoS conditions. Cisco addressed multiple vulnerabilities in IOS XR software as part of its semiannual Software Security Advisory Bundled Publication published on September 10, 2025.

Samsung fixed actively exploited zero-day

Security Affairs - 12 September 2025 12:44

Samsung fixed the remote code execution flaw CVE-2025-21043 that was exploited in zero-day attacks against Android devices. Samsung addressed the remote code execution vulnerability, tracked as CVE-2025-21043, that was exploited in zero-day attacks against Android users.

Critical CVE-2025-5086 in DELMIA Apriso Actively Exploited, CISA Issues Warning

The Hacker News - 12 September 2025 17:33

The U.S. Cybersecurity and Infrastructure Security Agency (CISA) on Thursday added a critical security flaw impacting Dassault Systèmes DELMIA Apriso Manufacturing Operations Management (MOM) software to its Known Exploited Vulnerabilities (KEV) catalog, based on evidence of active exploitation.

CISA: CVE Program to Focus on Vulnerability Data Quality

SecurityWeek - 12 September 2025 11:53

CISA says it is time for the CVE Program to focus on improving trust, responsiveness, and the caliber of vulnerability data.

Threat actors and malware

Scottish Cyber Coordination Centre

New VoidProxy phishing service targets Microsoft 365, Google accounts

BleepingComputer - 14 September 2025 11:23

A newly discovered phishing-as-a-service (PhaaS) platform, named VoidProxy, targets Microsoft 365 and Google accounts, including those protected by third-party single sign-on (SSO) providers such as Okta. [...]

New HybridPetya ransomware can bypass UEFI Secure Boot

BleepingComputer - 12 September 2025 14:18

A recently discovered ransomware strain called HybridPetya can bypass the UEFI Secure Boot feature to install a malicious application on the EFI System Partition. [...]

FBI warns of Salesforce attacks by UNC6040 and UNC6395 groups

Security Affairs - 13 September 2025 20:24

The U.S. FBI issued a flash alert to warn of malicious activities carried out by two cybercriminal groups tracked as UNC6040 and UNC6395. The FBI issued a FLASH alert with IOCs for cybercriminal groups UNC6040 and UNC6395, which are increasingly targeting Salesforce platforms for data theft and extortion.

HiddenGh0st, Winos and kkRAT Exploit SEO, GitHub Pages in Chinese Malware Attacks

The Hacker News - 15 September 2025 12:17

Chinese-speaking users are the target of a search engine optimization (SEO) poisoning campaign that uses fake software sites to distribute malware."The attackers manipulated search rankings with SEO plugins and registered lookalike domains that closely mimicked legitimate software sites,"

Attackers Adopting Novel LOTL Techniques to Evade Detection

Infosecurity Magazine - 12 September 2025 14:30

HP Wolf has reported the use of multiple, uncommon binaries and novel uses of legitimate image files in recent malicious campaigns

UK related

UK ICO finds students behind majority of school data breaches

Security Affairs - 15 September 2025 06:12

UK ICO reports students caused over half of school data breaches, showing kids are shaping cybersecurity in unexpected ways. The UK Information Commissioner's Office (ICO), students were responsible for most of the data breaches suffered by the schools in the country.

UK train operator LNER (London North Eastern Railway) discloses a data breach

Security Affairs - 12 September 2025 10:25

Scottish Cyber Coordination Centre

LNER warns of a data breach via a third-party supplier, exposing customer contact details and other personal information. UK train operator LNER (London North Eastern Railway) reported a data breach through a third-party supplier, compromising customer contact details and other personal information.