Scottish Cyber Coordination Centre

Daily Threat Bulletin

23 September 2025

Vulnerabilities

Microsoft Patches Critical Entra ID Flaw Enabling Global Admin Impersonation Across Tenants

The Hacker News - 22 September 2025 12:17

A critical token validation failure in Microsoft Entra ID (previously Azure Active Directory) could have allowed attackers to impersonate any user, including Global Administrators, across any tenant.The vulnerability, tracked as CVE-2025-55241, has been assigned the maximum CVSS score of 10.0. It has been described by Microsoft as a privilege escalation flaw in Azure Entra.

Fortra Patches Critical GoAnywhere MFT Vulnerability

SecurityWeek - 22 September 2025 08:50

Tracked as CVE-2025-10035 (CVSS score of 10), the critical deserialization vulnerability could be exploited for command injection.

Siemens OpenSSL Vulnerability in Industrial Products

CISA Advisories -

As of January 10, 2023, CISA will no longer be updating ICS security advisories for Siemens product vulnerabilities beyond the initial advisory.

Threat actors and malware

Airport disruptions in Europe caused by a ransomware attack

BleepingComputer - 22 September 2025 18:24

The disruptions over the weekend at several major European airports were caused by a ransomware attack targeting the check-in and boarding systems. [...]

Why attackers are moving beyond email-based phishing attacks

BleepingComputer - 22 September 2025 11:01

Phishing isn't just email anymore. Attackers now use social media, chat apps & malicious ads to steal credentials. Push Security explains the latest tactics and shows how to stop multi-channel phishing where it happens — inside the browser. [...]

Iran-Linked Hackers Target Europe With New Malware

darkreading - 22 September 2025 22:00

Scottish Cyber Coordination Centre

"Nimbus Manticore" is back at it, this time with improved variants of its flagship malware and targets that are outside its usual focus area.

Widespread Infostealer Campaign Targeting macOS Users

SecurityWeek - 22 September 2025 10:56

Threat actors rely on malicious GitHub repositories to infect LastPass's macOS users with the Atomic infostealer.

Organizations Must Update Defenses to Scattered Spider Tactics, Experts Urge

Infosecurity Magazine - 22 September 2025 17:10

Experts at a Gartner event highlighted areas of focus in identity, processes and third-party risk management to tackle the novel tactics employed by Scattered Spider