Scottish Cyber Coordination Centre

Daily Threat Bulletin

01 September 2025

Vulnerabilities

Microsoft fixes bug behind Windows certificate enrollment errors

BleepingComputer - 29 August 2025 15:02

Microsoft has resolved a known issue causing false CertificateServicesClient (CertEnroll) error messages after installing the July 2025 preview and subsequent Windows 11 24H2 updates.

Researchers Warn of Sitecore Exploit Chain Linking Cache Poisoning and Remote Code Execution

The Hacker News - 29 August 2025 23:52

Three new security vulnerabilities have been disclosed in the Sitecore Experience Platform that could be exploited to achieve information disclosure and remote code execution.

Click Studios Patches Passwordstate Authentication Bypass Vulnerability in Emergency Access Page

The Hacker News - 29 August 2025 16:28

Click Studios, the developer of enterprise-focused password management solution Passwordstate, said it has released security updates to address an authentication bypass vulnerability in its software.

FreePBX Servers Targeted by Zero-Day Flaw, Emergency Patch Now Available

The Hacker News - 29 August 2025 16:14

The Sangoma FreePBX Security Team has issued an advisory warning about an actively exploited FreePBX zero-day vulnerability that impacts systems with an administrator control panel (ACP) exposed to the public internet.

Enterprise password management outfit Passwordstate patches Emergency Access bug

The Register - 29 August 2025 14:13

Up to 29,000 organizations and potentially 370,000 security and IT pros affected Australian development house Click Studios has warned users of its Passwordstate enterprise password management platform to update immediately if not sooner, following the discovery of an authentication bypass vulnerability that opens the doors to an emergency administration account with nothing more than a “carefully crafted URL”.

Scottish Cyber Coordination Centre

Ransomware Group Exploits Hybrid Cloud Gaps, Gains Full Azure Control in Enterprise Attacks

SecurityWeek - 29 August 2025 13:10

Storm-0501 has been leveraging cloud-native capabilities for data exfiltration and deletion, without deploying file-encrypting malware. The post Ransomware Group Exploits Hybrid Cloud Gaps, Gains Full Azure Control in Enterprise Attacks appeared first on SecurityWeek.

Threat actors and malware

Attackers Abuse Velociraptor Forensic Tool to Deploy Visual Studio Code for C2 Tunneling

The Hacker News - 30 August 2025 18:36

Cybersecurity researchers have called attention to a cyber attack in which unknown threat actors deployed an open-source endpoint monitoring and digital forensic tool called Velociraptor, illustrating ongoing abuse of legitimate software for malicious purposes.

Amazon Disrupts APT29 Watering Hole Campaign Abusing Microsoft Device Code Authentication

The Hacker News - 29 August 2025 19:52

Amazon on Friday said it flagged and disrupted what it described as an opportunistic watering hole campaign orchestrated by the Russia-linked APT29 actors as part of their intelligence gathering efforts.

Malicious Actors Spread Malware Via Meta's Advertising System

Security Magazine - 29 August 2025 13:00

A Meta malvertising campaign has expanded to Android phones.

Google Confirms Workspace Accounts Also Hit in Salesforce–Salesloft Drift Data Theft Campaign

SecurityWeek - 29 August 2025 13:40

Google says the same OAuth token compromise that enabled Salesforce data theft also let hackers access a small number of Workspace accounts via the Salesloft Drift integration. The post Google Confirms Workspace Accounts Also Hit in Salesforce–Salesloft Drift Data Theft Campaign appeared first on SecurityWeek.

Nevada Confirms Ransomware Attack Behind Statewide Service Disruptions

SecurityWeek - 29 August 2025 13:28

State officials confirm ransomware forced office closures, disrupted services, and led to data theft, as Nevada works with CISA and law enforcement to restore critical systems.

Scottish Cyber Coordination Centre

Ransomware Group Exploits Hybrid Cloud Gaps, Gains Full Azure Control in Enterprise Attacks

SecurityWeek - 29 August 2025 13:10

Storm-0501 has been leveraging cloud-native capabilities for data exfiltration and deletion, without deploying file-encrypting malware.The post Ransomware Group Exploits Hybrid Cloud Gaps, Gains Full Azure Control in Enterprise Attacks appeared first on SecurityWeek.

UK related

How To Enact Meaningful Change This International Women in Cyber Day

Security Magazine - 01 September 2025 03:00

September 1st marks International Women in Cyber Day. While notable strides in progress have been made for women in the industry, there are still roadblocks that impede many career journeys.

AI-Powered Cybercrime Is Here: Massive Breaches & Dark Web Dumps

Security Boulevard - 31 August 2025 19:47

Cyber threats are escalating fast—and now AI is making them faster, smarter, and more dangerous than ever.

Phishing as a Service 2.0: The Franchise Model of Cybercrime

Security Boulevard - 30 August 2025 20:04

The Golden Arches of Malice When you think of franchising, you probably picture McDonald's, Starbucks, or Subway — not cybercriminals. But the uncomfortable truth is that modern cybercrime looks a lot less like "lone hacker in a hoodie" and a lot more like fast food chains.