Scottish Cyber Coordination Centre

Daily Threat Bulletin

9 July 2025

Vulnerabilities

Microsoft July 2025 Patch Tuesday fixes one zero-day, 137 flaws

BleepingComputer - 08 July 2025 14:30

Today is Microsoft's July 2025 Patch Tuesday, which includes security updates for 137 flaws, including one publicly disclosed zero-day vulnerability in Microsoft SQL Server.

Adobe Patches Critical Code Execution Bugs

SecurityWeek - 08 July 2025 22:22

Adobe patches were also released for medium-severity flaws in After Effects, Audition, Dimension, Experience Manager Screens, FrameMaker, Illustrator, Substance 3D Stager, and Substance 3D Viewer.

SAP Patches Critical Flaws That Could Allow Remote Code Execution, Full System Takeover

SecurityWeek - 08 July 2025 13:53

SAP has released patches for multiple insecure deserialization vulnerabilities in NetWeaver that could lead to full system compromise.

Malicious Pull Request Targets 6,000+ Developers via Vulnerable Ethcode VS Code Extension

The Hacker News - 08 July 2025 19:31

Cybersecurity researchers have flagged a supply chain attack targeting a Microsoft Visual Studio Code (VS Code) extension called Ethcode that has been installed a little over 6,000 times.

Threat actors and malware

Hackers Use Leaked Shellter Tool License to Spread Lumma Stealer and SectopRAT Malware

The Hacker News - 09 July 2025 00:05

In yet another instance of threat actors repurposing legitimate tools for malicious purposes, it has been discovered that hackers are exploiting a popular red teaming tool called Shellter to distribute stealer malware.

Scottish Cyber Coordination Centre

Massive browser hijacking campaign infects 2.3M Chrome, Edge users

The Register - 08 July 2025 20:07

A Chrome and Edge extension with more than 100,000 downloads that displays Google's verified badge does what it purports to do: It delivers a color picker to users. Unfortunately, it also hijacks every browser session, tracks activities across websites, and backdoors victims' web browsers.

New Android TapTrap attack fools users with invisible UI trick

BleepingComputer - 08 July 2025 16:39

A novel tapjacking technique can exploit user interface animations to bypass Android's permission system and allow access to sensitive data or trick users into performing destructive actions, such as wiping the device.

Over 500 Scattered Spider Phishing Domains Poised to Target Multiple Industries

Infosecurity Magazine - 08 July 2025 14:00

Check Point discovered around 500 suspected Scattered Spider phishing domains, suggesting the group is preparing to expand its targeting

New Bert Ransomware Evolves With Multiple Variants

Security Boulevard - 08 July 2025 16:36

An emerging ransomware group that calls itself Bert is quickly evolving after hitting the cybercrime scene in April, targeting both Windows and Linux systems used by organizations in the health care, tech, and other industries in the United States, Europe, and Asia.