Scottish
Cyber
Coordination
Centre

Daily Threat Bulletin

10 September 2025

Vulnerabilities

Microsoft September 2025 Patch Tuesday fixes 81 flaws, two zero-days

BleepingComputer - 09 September 2025 14:43

Today is Microsoft's September 2025 Patch Tuesday, which includes security updates for 81 flaws, including two publicly disclosed zero-day vulnerabilities. [...]

Adobe patches critical SessionReaper flaw in Magento eCommerce platform

BleepingComputer - 09 September 2025 12:53

Adobe is warning of a critical vulnerability (CVE-2025-54236) in its Commerce and Magento Open Source platforms that researchers call SessionReaper and describe as one of " the most severe" flaws in the history of the product. [...]

SAP Patches Critical NetWeaver (CVSS Up to 10.0) and High-Severity S/4HANA Flaws

The Hacker News - 10 September 2025 07:33

SAP on Tuesday released security updates to address multiple security flaws, including three critical vulnerabilities in SAP Netweaver that could result in code execution and the upload arbitrary files.The vulnerabilities are listed below -CVE-2025-42944 (CVSS score: 10.0)

Microsoft Patches 86 Vulnerabilities

SecurityWeek - 09 September 2025 19:44

Microsoft has released patches for dozens of flaws in Windows and other products, including ones with 'exploitation more likely' rating.

Exposed Docker APIs Likely Exploited to Build Botnet

SecurityWeek - 09 September 2025 15:01

Hackers mount the host's file system into fresh containers, fetch malicious scripts over the Tor network, and block access to the Docker API.

Threat actors and malware

Supply chain attack targets npm, +2 Billion weekly npm downloads exposed

Security Affairs - 09 September 2025 19:26

Multiple popular npm packages were compromised in a supply chain attack after a maintainer fell for a phishing email targeting 2FA credentials. A supply chain attack compromised multiple popular npm packages with 2B weekly downloads after a maintainer fell for a phishing email mimicking npm, targeting 2FA credentials. Threat actors targeted Josh Junon’s (Qix) to [...]

Axios Abuse and Salty 2FA Kits Fuel Advanced Microsoft 365 Phishing Attacks

The Hacker News - 09 September 2025 20:44

Threat actors are abusing HTTP client tools like Axios in conjunction with Microsoft’s Direct Send feature to form a “highly efficient attack pipeline” in recent phishing campaigns, according to new findings from ReliaQuest.

RatOn Android Malware Detected With NFC Relay and ATS Banking Fraud Capabilities

The Hacker News - 09 September 2025 18:23

A new Android malware called RatOn has evolved from a basic tool capable of conducting Near Field Communication (NFC) relay attacks to a sophisticated remote access trojan with Automated Transfer System (ATS) capabilities to conduct device fraud.

From MostereRAT to ClickFix: New Malware Campaigns Highlight Rising AI and Phishing Risks

The Hacker News - 09 September 2025 16:57

Cybersecurity researchers have disclosed details of a phishing campaign that delivers a stealthy banking malware-turned-remote access trojan called MostereRAT.The phishing attack incorporates a number of advanced evasion techniques to gain complete control over compromised systems, siphon sensitive data, and extend its functionality by serving secondary plugins, Fortinet FortiGuard Labs said.”

Russian Threat Group Targets Microsoft Outlook With Malware

Security Magazine - 09 September 2025 11:00

Research has identified a new Outlook backdoor linked to a Russian-linked persistent threat group.

Threat Actor Connected to Play, RansomHub and DragonForce Ransomware Operations

SecurityWeek - 09 September 2025 11:36

The attacker deployed multiple malware families, including two backdoors and a proxy tunneller, and various reconnaissance tools.