

Daily Threat Bulletin

11 July 2025

Vulnerabilities

[ServiceNow Flaw CVE-2025-3648 Could Lead to Data Exposure via Misconfigured ACLs](#)

The Hacker News - 10 July 2025 13:54

A high-severity security flaw has been disclosed in ServiceNow's platform that, if successfully exploited, could result in data exposure and exfiltration. The vulnerability, tracked as CVE-2025-3648 (CVSS score: 8.2), has been described as a case of data inference in Now Platform through conditional access control list (ACL) rules.

[CISA Adds One Known Exploited Vulnerability to Catalog](#)

CISA Advisories -

CISA has added one new vulnerability to its Known Exploited Vulnerabilities (KEV) Catalog, based on evidence of active exploitation. CVE-2025-5777 Citrix NetScaler ADC and Gateway Out-of-Bounds Read Vulnerability

[Critical mcp-remote Vulnerability Enables Remote Code Execution, Impacting 437,000+ Downloads](#)

The Hacker News - 10 July 2025 23:33

Cybersecurity researchers have discovered a critical vulnerability in the open-source mcp-remote project that could result in the execution of arbitrary operating system (OS) commands. The vulnerability, tracked as CVE-2025-6514, carries a CVSS score of 9.6 out of 10.0.

[PerfektBlue Bluetooth flaws impact Mercedes, Volkswagen, Skoda cars](#)

BleepingComputer - 10 July 2025 13:01

Four vulnerabilities dubbed PerfektBlue and affecting the BlueSDK Bluetooth stack from OpenSynergy can be exploited to achieve remote code execution and potentially allow access to critical elements in vehicles from multiple vendors, including Mercedes-Benz AG, Volkswagen, and Skoda.

Threat actors and malware

[New ZuRu Malware Variant Targeting Developers via Trojanized Termius macOS App](#)

The Hacker News - 10 July 2025 17:29

Cybersecurity researchers have discovered new artifacts associated with an Apple macOS malware called ZuRu, which is known to propagate via trojanized versions of legitimate software.



Scottish
Cyber
Coordination
Centre

eSIM Hack Allows for Cloning, Spying

SecurityWeek - 10 July 2025 15:21

Details have been disclosed for an eSIM hacking method that could impact many, but the industry is taking action.

UK incidents

Four arrested in UK over M&S, Co-op, Harrod cyberattacks

BleepingComputer - 10 July 2025 10:46

The UK's National Crime Agency (NCA) arrested four people suspected of being involved in cyberattacks on major retailers in the country, including Marks & Spencer, Co-op, and Harrods.