Scottish
Cyber
Coordination
Centre

Daily Threat Bulletin

2 July 2025

Vulnerabilities

Critical Vulnerability in Anthropic’s MCP Exposes Developer Machines to Remote Exploits

The Hacker News - 02 July 2025 00:33

Cybersecurity researchers have discovered a critical security vulnerability in artificial intelligence (AI) company Anthropic’s Model Context Protocol (MCP) Inspector project that could result in remote code execution (RCE) and allow an attacker to gain complete access to the hosts.

New Flaw in IDEs Like Visual Studio Code Lets Malicious Extensions Bypass Verified Status

The Hacker News - 01 July 2025 20:21

A new study of integrated development environments (IDEs) like Microsoft Visual Studio Code, Visual Studio, IntelliJ IDEA, and Cursor has revealed weaknesses in how they handle the extension verification process, ultimately enabling attackers to execute malicious code on developer machines.

Update your Chrome to fix new actively exploited zero-day vulnerability

Malwarebytes - 01 July 2025 16:12

Google has released an urgent update for the Chrome browser to patch a vulnerability which has already been exploited.

Bluetooth vulnerability in audio devices can be exploited to spy on users

Malwarebytes - 01 July 2025 15:57

Researchers have found a set of vulnerabilities in Bluetooth connected devices that could allow an attacker to spy on users.

CISA Adds Two Known Exploited Vulnerabilities to Catalog

CISA Advisories -

CISA has added two new vulnerabilities to its Known Exploited Vulnerabilities (KEV) Catalog, based on evidence of active exploitation. CVE-2025-48927 TeleMessage TM SGNL Initialization of a Resource with an Insecure Default Vulnerability, CVE-2025-48928 TeleMessage TM SGNL Exposure of Core Dump File to an Unauthorized Control Sphere Vulnerability

Threat actors and malware

New FileFix attack runs JScript while bypassing Windows MoTW alerts

BleepingComputer - 01 July 2025 13:37

A new FileFix attack allows executing malicious scripts while bypassing the Mark of the Web (MoTW) protection in Windows by exploiting how browsers handle saved HTML webpages. [...]

CISA and U.S. Agencies warn of ongoing Iranian cyber threats to critical infrastructure

Security Affairs - 01 July 2025 08:15

U.S. warns of rising Iranian cyber threats exploiting outdated software and weak passwords, with attacks likely to escalate due to recent events. U.S. cybersecurity and intelligence agencies warn of rising cyber threats from Iranian state-linked hackers, expected to escalate. These actors typically exploit outdated software, known vulnerabilities, and weak or default passwords on internet-connected systems. [...]

TA829 and UNK_GreenSec Share Tactics and Infrastructure in Ongoing Malware Campaigns

The Hacker News - 01 July 2025 22:56

Cybersecurity researchers have flagged the tactical similarities between the threat actors behind the RomCom RAT and a cluster that has been observed delivering a loader dubbed TransferLoader.Enterprise security firm Proofpoint is tracking the activity associated with TransferLoader to a group dubbed UNK_GreenSec and the RomCom RAT actors under the moniker TA829.

International Criminal Court swats away ‘sophisticated and targeted’ cyberattack

The Register - 01 July 2025 17:34

Body stays coy on details but alludes to similarities with 2023 espionage campaign The International Criminal Court (ICC) says a “sophisticated” cyberattack targeted the institution, the second such incident in two years.

New Report Uncovers Major Overlaps in Cybercrime and State-Sponsored Espionage

Infosecurity Magazine - 01 July 2025 15:30

Proofpoint has identified similarities between the tactics of a pro-Russian cyber espionage group and a cybercriminal gang