Scottish
Cyber
Coordination
Centre

Daily Threat Bulletin

26 March 2025

Vulnerabilities

Zero-Day Alert: Google Releases Chrome Patch for Exploit Used in Russian Espionage Attacks

The Hacker News - 26 March 2025 11:26

Google has released out-of-band fixes to address a high-severity security flaw in its Chrome browser for Windows that it said has been exploited in the wild as part of attacks targeting organizations in Russia. The vulnerability, tracked as CVE-2025-2783, has been described as a case of incorrect handle provided in unspecified circumstances in Mojo on Windows.

CrushFTP warns users to patch unauthenticated access flaw immediately

BleepingComputer - 25 March 2025 17:11

CrushFTP warned customers of an unauthenticated HTTP(S) port access vulnerability and urged them to patch their servers immediately.

VMware Patches Authentication Bypass Flaw in Windows Tools Suite

SecurityWeek - 25 March 2025 16:01

The authentication bypass vulnerability, tagged as CVE-2025-22230, carries a CVSS severity score of 7.8/10.

New Windows zero-day leaks NTLM hashes, gets unofficial patch

BleepingComputer - 25 March 2025 15:22

Free unofficial patches are available for a new Windows zero-day vulnerability that can let remote attackers steal NTLM credentials by tricking targets into viewing malicious files in Windows Explorer.

Vulnerability Exploitation Possibly Behind Widespread DrayTek Router Reboots

SecurityWeek - 25 March 2025 16:21

DrayTek routers around the world are rebooting and the vendor’s statement suggests that it may involve the exploitation of a vulnerability.

Threat actors and malware

EncryptHub linked to MMC zero-day attacks on Windows systems

BleepingComputer - 25 March 2025 13:51

A threat actor known as EncryptHub has been linked to Windows zero-day attacks exploiting a Microsoft Management Console vulnerability patched this month.

Android malware campaigns use .NET MAUI to evade detection

Security Affairs - 25 March 2025 19:55

McAfee researchers warn of Android malware campaigns using .NET MAUI to evade detection. These threats disguise themselves as legitimate services to steal sensitive information from users.

Cybercriminals Use Atlantis AIO to Target 140+ Platforms

Infosecurity Magazine - 25 March 2025 17:30

Cybercriminals are increasingly leveraging Atlantis AIO, which automates credential stuffing attacks across more than 140 platforms.

UK incidents

There are perhaps 10,000 reasons to doubt Oracle Cloud’s security breach denial

The Register - 25 March 2025 18:35

Customers come forward claiming info was swiped from prod Oracle Cloud’s denial of a digital break-in is now in clear dispute. An infosec researcher working on validating claims that the cloud provider’s login servers were compromised earlier this year says some customers have confirmed data allegedly stolen and leaked from the database giant is genuine.