Scottish Cyber Coordination Centre

Daily Threat Bulletin

26 June 2025

Vulnerabilities

Citrix warns of NetScaler vulnerability exploited in DoS attacks

BleepingComputer - 25 June 2025 14:35

Citrix is warning that a vulnerability in NetScaler appliances tracked as CVE-2025-6543 is being actively exploited in the wild, causing devices to enter a denial of service condition.

Citrix Bleed 2 Flaw Enables Token Theft; SAP GUI Flaws Risk Sensitive Data Exposure

The Hacker News - 25 June 2025 20:07

Cybersecurity researchers have detailed two now-patched security flaws in SAP Graphical User Interface (GUI) for Windows and Java that, if successfully exploited, could have enabled attackers to access sensitive information under certain conditions.

WinRAR patches bug letting malware launch from extracted archives

BleepingComputer - 25 June 2025 13:55

WinRAR has addressed a directory traversal vulnerability tracked as CVE-2025-6218 that, under certain circumstances, allows malware to be executed after extracting a malicious archive.

Millions of Brother Printers Hit by Critical, Unpatchable Bug

darkreading - 25 June 2025 19:57

A slew of vulnerabilities, including a critical CVSS 9.8 that enables an attacker to generate the default admin password, affect hundreds of printer, scanner, and label-maker models made by manufacturer Brother.

Code Execution Vulnerability Patched in GitHub Enterprise Server

SecurityWeek - 25 June 2025 11:42

A high-severity vulnerability in GitHub Enterprise Server could have allowed remote attackers to execute arbitrary code.

Microsoft nOAuth Flaw Still Exposes SaaS Apps Two Years After Discovery

Infosecurity Magazine - 25 June 2025 14:30

Semperis estimates that at least 15,000 enterprise SaaS applications are still vulnerable to a flaw discovered in 2023.

Scottish Cyber Coordination Centre

Chrome 138, Firefox 140 Patch Multiple Vulnerabilities

SecurityWeek - 25 June 2025 11:02

Chrome 138 and Firefox 140 are rolling out with fixes for two dozen vulnerabilities, including high-severity memory safety issues.

CISA Adds Three Known Exploited Vulnerabilities to Catalog

CISA Advisories -

CISA has added three new vulnerabilities to its Known Exploited Vulnerabilities (KEV) Catalog, based on evidence of active exploitation:
CVE-2024-54085 - AMI MegaRAC SPx Authentication Bypass by Spoofing Vulnerability.
CVE-2024-0769 - D-Link DIR-859 Router Path Traversal Vulnerability.
CVE-2019-6693 - Fortinet FortiOS Use of Hard-Coded Credentials Vulnerability.

Threat actors and malware

Hackers turn ScreenConnect into malware using Authenticode stuffing

BleepingComputer - 25 June 2025 18:51

Threat actors are abusing the ConnectWise ScreenConnect installer to build signed remote access malware by modifying hidden settings within the client's Authenticode signature.

Hackers deploy fake SonicWall VPN App to steal corporate credentials

Security Affairs - 25 June 2025 19:09

Unknown threat actors are distributing a trojanized version of SonicWall NetExtender SSL VPN app to steal user credentials.

Hackers abuse Microsoft ClickOnce and AWS services for stealthy attacks

BleepingComputer - 25 June 2025 17:34

A sophisticated malicious campaign that researchers call OneClik has been leveraging Microsoft's ClickOnce software deployment tool and custom Golang backdoors to compromise organizations within the energy, oil, and gas sectors.

Hacker 'IntelBroker' charged in US for global data theft breaches

BleepingComputer - 25 June 2025 20:54

A British national known online as "IntelBroker" has been charged by the U.S. for stealing and selling sensitive data from dozens of victims, causing an estimated $25 million in damages.

Scottish Cyber Coordination Centre

UK incidents

Data theft fears after cyber attack on Glasgow City Council

BBC News - 25 June 2025 13:45

The local authority said it was targeted on Thursday and customer data may have been stolen. A number of online services, including paying penalty charges and reporting school absences, are unavailable due to the council taking servers offline.

Ransomware attack contributed to patient's death, says Britain's NHS

The Record from Recorded Future News - 25 June 2025 15:21

A ransomware attack that disrupted blood testing across several hospitals in London last year contributed to a patients death, according to the National Health Service.

UK Ransom Payments Double as Victims Fall Behind Global Peers

Infosecurity Magazine - 25 June 2025 10:45

British organizations are far more likely than their global peers to have data encrypted in ransomware attacks, and to pay a higher ransom demand, according to Sophos.