Scottish
Cyber
Coordination
Centre

Daily Threat Bulletin

23 July 2025

Vulnerabilities

Cisco: Maximum-severity ISE RCE flaws now exploited in attacks

BleepingComputer - 22 July 2025 11:40

Cisco is warning that three recently patched critical remote code execution vulnerabilities in Cisco Identity Services Engine (ISE) are now being actively exploited in attacks.

Vulnerabilities Expose Helmholz Industrial Routers to Hacking

SecurityWeek - 22 July 2025 14:50

Eight vulnerabilities, including ones allowing full control over a device, have been discovered and patched in Helmholz REX 100 industrial routers.

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-2025-49704 Microsoft SharePoint Code Injection Vulnerability & CVE-2025-49706 Microsoft SharePoint Improper Authentication Vulnerability.

UPDATE: Microsoft Releases Guidance on Exploitation of SharePoint Vulnerabilities

CISA Advisories -

Update (07/22/2025): This Alert was updated to reflect newly released information from Microsoft, and to correct the actively exploited Common Vulnerabilities and Exposures (CVEs), which have been confirmed as CVE-2025-49706, a network spoofing vulnerability, and CVE-2025-49704, a remote code execution (RCE) vulnerability.

Threat actors and malware

Microsoft Says Chinese APTs Exploited ToolShell Zero-Days Weeks Before Patch

SecurityWeek - 22 July 2025 18:41

Microsoft says the Chinese threat actors Linen Typhoon, Violet Typhoon, and Storm-2603 have been exploiting the ToolShell zero-days.

Lumma infostealer malware returns after law enforcement disruption

BleepingComputer - 22 July 2025 18:34

The Lumma infostealer malware operation is gradually resuming activities following a massive law enforcement operation in May, which resulted in the seizure of 2,300 domains and parts of its infrastructure.

Coyote malware abuses Windows accessibility framework for data theft

BleepingComputer - 22 July 2025 14:54

A new variant of the banking trojan 'Coyote' has begun abusing a Windows accessibility feature, Microsoft's UI Automation framework, to identify which banking and cryptocurrency exchange sites are accessed on the device for potential credential theft.

Joint Advisory Issued on Protecting Against Interlock Ransomware

CISA Advisories -

CISA, in partnership with the Federal Bureau of Investigation (FBI), the Department of Health and Human Services, and the Multi-State Information Sharing and Analysis Center issued a joint Cybersecurity Advisory to help protect businesses and critical infrastructure organizations in North America and Europe against Interlock ransomware

UK incidents

UK Confirms Ransomware Payment Ban for Public Sector and CNI

Infosecurity Magazine - 22 July 2025 13:30

The UK government said a public consultation showed widespread support on a payment ban for public sector and CNI organizations