Scottish Cyber Coordination Centre

Daily Threat Bulletin

27 July 2026

Vulnerabilities

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-2026-16232 Check Point SmartConsole Improper Authentication Vulnerability.

CVE-2026-50522 Microsoft SharePoint Deserialization of Untrusted Data Vulnerability.

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-2026-25089 Fortinet FortiSandbox OS Command Injection Vulnerability.

CVE-2026-39808 Fortinet FortiSandbox OS Command Injection Vulnerability.

CVE-2026-58644 Microsoft SharePoint Deserialization of Untrusted Data Vulnerability.

Threat actors and malware

Hackers Hijack Hotel Wi-Fi to Steal Microsoft 365 Credentials

Security Affairs - 26 July 2026 14:04

Hackers compromised hotel Wi-Fi gateways to redirect users to fake Microsoft 365 login pages and steal credentials. ReliaQuest's threat research team just documented attackers compromising the Wi-Fi gateways at hotels and conference centers.

Russian State-Supported Cyber Actors Conduct Phishing Campaign Targeting Users of Zimbra Collaboration Suite

CISA Advisories -

Russian State-Supported Cyber Actors Conduct Phishing Campaign Targeting Users of Zimbra Collaboration SuiteExecutive summary. A group of Russian state-supported cyber actors has been targeting and compromising various Western government and commercial organizations using the Zimbra Collaboration Suite (ZCS) software since at least July 2025.

Scottish Cyber Coordination Centre

Rockwell Automation FactoryTalk Services Platform

CISA Advisories -

Successful exploitation of this vulnerability could allow an attacker to impersonate an authorized user on the FTSP server, resulting in unauthorized access to system configurations.

UK related

Policies and procedures required by ISO 27001: a practical guide for UK SMEs

Security Boulevard - 27 July 2026 03:23

Policies and procedures required by ISO 27001: A practical guide for UK SMEs If you are trying to build an ISO 27001-aligned information security management system, the first question is usually not about technology.