Scottish Cyber Coordination Centre

Daily Threat Bulletin

14 April 2026

Vulnerabilities

CC-4769 - Adobe Releases Security Update to Address a Vulnerability in Acrobat and Reader

NHS Digital - 13 April 2026 14:37

Severity: Medium CVE-2026-34621 could allow arbitrary code execution via malicious PDF files opened in vulnerable Adobe Acrobat or Reader installations. CVE-2026-34621 could allow arbitrary code execution via malicious PDF files opened in vulnerable Adobe Acrobat or Reader installations.

Critical flaw in wolfSSL library enables forged certificate use

BleepingComputer - 13 April 2026 16:56

A critical vulnerability in the wolfSSL SSL/TLS library can weaken security via improper verification of the hash algorithm or its size when checking Elliptic Curve Digital Signature Algorithm (ECDSA) signatures. [...]

ShowDoc RCE Flaw CVE-2025-0520 Actively Exploited on Unpatched Servers

The Hacker News - 14 April 2026 12:20

A critical security vulnerability impacting ShowDoc, a document management and collaboration service popular in China, has come under active exploitation in the wild.

CISA Adds Seven Known Exploited Vulnerabilities to Catalog

CISA Advisories -

CISA has added seven new vulnerabilities to its Known Exploited Vulnerabilities (KEV) Catalog, based on evidence of active exploitation: CVE-2012-1854 Microsoft Visual Basic for Applications Insecure Library Loading Vulnerability; CVE-2020-9715 Adobe Acrobat Use-After-Free Vulnerability; CVE-2023-21529 Microsoft Exchange Server Deserialization of Untrusted Data Vulnerability; CVE-2023-36424 Microsoft Windows Out-of-Bounds Read Vulnerability; CVE-2025-60710 Microsoft Windows Link Following Vulnerability; CVE-2026-21643 Fortinet SQL Injection Vulnerability; CVE-2026-34621 Adobe Acrobat and Reader Prototype Pollution Vulnerability. These types of vulnerabilities are frequent attack vectors for malicious cyber actors and pose significant risks to the federal enterprise.

Threat actors and malware

OpenAI rotates macOS certs after Axios attack hit code-signing workflow

BleepingComputer - 13 April 2026 14:39

OpenAI is rotating potentially exposed macOS code-signing certificates after a GitHub Actions workflow executed a malicious Axios package during a recent supply chain attack. [...]

CPUID watering hole attack spreads STX RAT malware

Security Affairs - 13 April 2026 08:23

Threat actors compromised the CPUID website and spread STX RAT through fake CPU-Z and HWMonitor downloads. Attackers breached the website CPUID and replaced download links for CPU-Z and HWMonitor with malicious files for several hours. Users who downloaded them got infected with the STX RAT, giving attackers remote access to their systems. The short attack [...]

Mailbox Rule Abuse Emerges as Stealthy Post-Compromise Threat

Infosecurity Magazine - 13 April 2026 16:00

Attackers are abusing Microsoft 365 mailbox rules to hide activity, exfiltrate data and retain access after account compromise, researchers warn

Iranian-Affiliated Cyber Actors Exploit Programmable Logic Controllers Across US Critical Infrastructure

CISA Advisories -

Iranian-Affiliated Cyber Actors Exploit Programmable Logic Controllers Across US Critical InfrastructureOriginal PublicationApril 7, 2026Executive SummaryIran-affiliated advanced persistent threat (APT) actors are conducting exploitation activity targeting internet-facing operational technology (OT) devices, including programmable logic controllers (PLCs) manufactured by Rockwell Automation/Allen-Bradley.

UK related

UK Cyber Security Council Launches Associate Cyber Security Professional Title

Infosecurity Magazine - 13 April 2026 10:15

The UK Cyber Security Council has unveiled a new Associate Cyber Security Professional title aimed at supporting early-career cybersecurity professionals