Scottish Cyber Coordination Centre

Daily Threat Bulletin

18 May 2026

Vulnerabilities

CISA Adds One Known Exploited Vulnerability to Catalog

CISA Advisories -

CISA has added one new vulnerability to its Known Exploited Vulnerabilities (KEV) Catalog, based on evidence of active exploitation. CVE-2026-42897 Microsoft Exchange Server Cross-Site Scripting Vulnerability.

CC-4785 - Microsoft Releases Security Advisory for a Zero-Day Vulnerability in Exchange Server

NHS Digital - 15 May 2026 11:56

Severity: Medium Successful exploitation of CVE-2026-42897 could lead to arbitrary JavaScript execution in the browser context for users of on-premises Microsoft Exchange Server deployments Successful exploitation of CVE-2026-42897 could lead to arbitrary JavaScript execution in the browser context for users of on-premises Microsoft Exchange Server deployments

CC-4784 - Exploitation of Zero-Day Vulnerability in Cisco Catalyst SD-WAN

NHS Digital - 15 May 2026 10:50

Severity: High CVE-2026-20182 could allow an unauthenticated attacker to bypass authentication and gain administrative privileges CVE-2026-20182 could allow an unauthenticated attacker to bypass authentication and gain administrative privileges

New Windows 'MiniPlasma' zero-day exploit gives SYSTEM access, PoC released

BleepingComputer - 17 May 2026 19:30

A cybersecurity researcher has released a proof-of-concept exploit for a Windows privilege escalation zero-day dubbed "MiniPlasma" that lets attackers gain SYSTEM privileges on fully patched Windows systems. [...]

Microsoft rejects critical Azure vulnerability report, no CVE issued

BleepingComputer - 16 May 2026 17:55

A security researcher claims Microsoft quietly fixed an Azure Backup for AKS vulnerability after rejecting his report, and without issuing a CVE. Microsoft disputes the claim, telling BleepingComputer the behavior was expected and that "no product changes were made," despite the researcher documenting a silent fix. [...]

Avada Builder WordPress plugin flaws allow site credential theft

BleepingComputer - 15 May 2026 12:56

Two vulnerabilities in the Avada Builder plugin for WordPress, with an estimated one million active installations, allow hackers to read arbitrary files and extract sensitive information from the database. [...]

Funnel Builder Flaw Under Active Exploitation Enables WooCommerce Checkout Skimming

The Hacker News - 16 May 2026 21:50

A critical security vulnerability impacting the Funnel Builder plugin for WordPress has come under active exploitation in the wild to inject malicious JavaScript code into WooCommerce checkout pages with the goal of stealing payment data.

Threat actors and malware

Russian hackers turn Kazuar backdoor into modular P2P botnet

BleepingComputer - 16 May 2026 11:15

The Russian hacker group Secret Blizzard has developed its long-running Kazuar backdoor into a modular peer-to-peer (P2P) botnet designed for long-term persistence, stealth, and data collection. [...]

OpenAI hit by supply chain attack linked to malicious TanStack packages

Security Affairs - 16 May 2026 10:31

OpenAI said the TanStack supply chain attack compromised two employee devices and exposed credentials from code repositories. OpenAI confirmed that the recent TanStack supply chain attack compromised two employee devices and exposed credential material stored in internal source code repositories.

Gremlin Stealer Evolves into Modular Threat with Advanced Evasion Capabilities

Infosecurity Magazine - 15 May 2026 15:19

A new Gremlin stealer variant has evolved into a modular toolkit with advanced evasion and data theft capabilities, according to new Unit 42 research

China-Linked Hackers Deploy New TencShell Malware Against Global Manufacturer

Infosecurity Magazine - 15 May 2026 09:00

A suspected China-linked threat actor targeted the Indian branch of a global manufacturer leveraging an open source offensive toolkit

Attackers replaced JDownloader installer downloads with malware

Malwarebytes - 15 May 2026 13:45

The JDownloader website was compromised and installer download links served malware for several days.

Scottish
Cyber
Coordination
Centre