Scottish Cyber Coordination Centre

Daily Threat Bulletin

21 July 2026

Vulnerabilities

CC-4817 - F5 Releases Security Advisory for Critical Vulnerability in NGINX and NGINX Plus

NHS Digital - 20 July 2026 14:06

Severity: Medium Successful exploitation of CVE-2026-42533 could allow an unauthenticated remote attacker to cause a denial-of-service condition or potentially achieve remote code execution on a targeted system.

CC-4816 - Exploitation of Critical Vulnerability in Microsoft SharePoint Server

NHS Digital - 20 July 2026 12:00

Severity: High Successful exploitation of CVE-2026-58644 could allow an unauthenticated attacker to execute code remotely Successful exploitation of CVE-2026-58644 could allow an unauthenticated attacker to execute code remotely Updated: 20 Jul 2026

CC-4815 - Critical Vulnerability Chain in WordPress Core Under Exploitation (wp2shell)

NHS Digital - 20 July 2026 11:35

Severity: High Successful exploitation of CVE-2026-63030 and CVE-2026-60137 could allow an unauthenticated attacker to execute code remotely Successful exploitation of CVE-2026-63030 and CVE-2026-60137 could allow an unauthenticated attacker to execute code remotely Updated: 20 Jul 2026

SonicWall SMA1000 flaws exploited as zero-days to push custom malware

BleepingComputer - 20 July 2026 19:23

Two recently disclosed SonicWall SMA1000 vulnerabilities were exploited in zero-day attacks for weeks, allowing threat actors to install custom malware on vulnerable VPN appliances. [...]

Critical 7-Zip Flaw Allows Code Execution by Opening Crafted XZ-Compressed Files. Update it now!

Security Affairs - 20 July 2026 11:56

7-Zip fixed a vulnerability that could let attackers run code by tricking users into opening malicious XZ-compressed archive files. 7-Zip released version 26.02 to address a remote code execution vulnerability in its handling of XZ-compressed data.

CVE-2026-42533: Critical NGINX Bug Could Turn HTTP Requests Into Server Takeovers

Security Affairs - 20 July 2026 10:50

Scottish Cyber Coordination Centre

F5 fixes critical nginx flaw CVE-2026-42533 that can crash servers and, in some cases, allow remote code execution through crafted HTTP requests.

Threat actors and malware

JadePuffer agentic attacks now target AI model data with ransomware

BleepingComputer - 20 July 2026 18:08

The JadePuffer autonomous AI agent has upgraded with custom malware called EncForge that focuses on encrypting AI assets, such as training datasets, vector databases, and model checkpoints. [...]

New HollowGraph malware uses Microsoft Graph for stealthy C2 comms

BleepingComputer - 20 July 2026 14:43

A malicious component dubbed HollowGraph uses the calendar feature in compromised Microsoft 365 mailboxes as a command-and-control channel to receive attacker commands and exfiltrate stolen data. [...]

Volexity Uncovers Zero-Day Campaign Targeting SonicWall VPN Appliances

Security Affairs - 20 July 2026 08:29

Unknown hackers exploited two SonicWall SMA 1000 zero-days to gain root access on VPN appliances before patches became available.

FakeGit Campaign Uses 7,600 GitHub Repositories to Spread SmartLoader Malware

The Hacker News - 21 July 2026 00:53

Cybersecurity researchers have discovered nearly 7,600 malicious GitHub repositories, out of which more than 800 pose as artificial intelligence (AI) skills or Model Context Protocol (MCP) servers to deliver a malware family known as SmartLoader as part of an ongoing campaign codenamed FakeGit.

Exposed Server Reveals AI-Assisted Phishing Toolkit Behind WebDAV Malware Campaign

The Hacker News - 20 July 2026 23:59

A malware operator left its delivery server wide open, and Rapid7 pulled down the whole toolkit: 1,048 files spanning lure templates, filename-spoofing tests, execution experiments, droppers, builder notes, and two campaign chains.