Scottish Cyber Coordination Centre

Daily Threat Bulletin

22 July 2026

Vulnerabilities

Public PoC triggers active exploitation of critical SharePoint RCE vulnerability CVE-2026-50522

Security Affairs - 21 July 2026 22:38

A critical Microsoft SharePoint vulnerability, tracked as CVE-2026-50522 (CVSS score of 9.8), is being actively exploited following the release of a public proof-of-concept (PoC) code, according to watchTowr researchers.

Critical wp2shell WordPress flaws exploited to install webshells

BleepingComputer - 21 July 2026 13:41

Hackers are exploiting the “wp2shell” critical vulnerability suite (CVE-2026-63030 and CVE-2026-60137) affecting WordPress Core to deploy persistent webshells and install malicious plugins on affected servers.

CISA Adds Four Known Exploited Vulnerabilities to Catalog

CISA Advisories -

CISA has added four new vulnerabilities to its Known Exploited Vulnerabilities (KEV) Catalog, based on evidence of active exploitation.

CVE-2021-27137 DD-WRT Stack-Based Buffer Overflow Vulnerability

CVE-2026-0770 Langflow Inclusion of Functionality from Untrusted Control Sphere Vulnerability

CVE-2026-63030 WordPress Core Interpretation Conflict Vulnerability

CVE-2026-60137 WordPress Core SQL Injection Vulnerability

Qilin Ransomware Affiliates Abuse CVE-2026-0257 to Gain Unauthorized VPN Access

Security Affairs - 21 July 2026 17:08

Arctic Wolf researchers warn that the Qilin ransomware gang is exploiting the critical PAN-OS GlobalProtect vulnerability CVE-2026-0257 to compromise corporate networks. CVE-2026-0257 is a PAN-OS authentication bypass vulnerability affecting GlobalProtect portals and gateways.

Scottish Cyber Coordination Centre

Critical ServiceNow AI Platform Flaw Exploited for Unauthenticated Code Execution

The Hacker News - 21 July 2026 12:59

Threat actors are now exploiting a recently disclosed critical security flaw impacting ServiceNow AI Platform, according to Defused Cyber. In a post shared on X, the threat intelligence firm said it's observing in-the-wild exploitation of CVE-2026-6875 (CVSS score: 9.5), a sandbox escape vulnerability that could allow an unauthenticated user to run arbitrary code.

Microsoft Azure DevOps MCP Flaw Lets Hidden PR Comments Hijack AI Review Agents

The Hacker News - 22 July 2026 11:27

A single invisible comment in an Azure DevOps pull request can turn a reviewer's own AI coding agent against them, driving it into projects the attacker has no rights to reach and quietly leaking what it finds.

Zimbra 10.1.20 patches multiple security issues, including a critical command injection bug

Security Affairs - 21 July 2026 19:25

Zimbra released version 10.1.20 to fix nine security vulnerabilities, including a critical command injection flaw in the SNMP monitoring component. The vulnerability affects systems with SNMP notifications enabled and could allow attackers to execute arbitrary commands.

Threat actors and malware

New ENCFORGE Ransomware Targets AI Model Files in Langflow RCE Attack

The Hacker News - 21 July 2026 14:04

Researchers at Sysdig have linked a second attack on the same Langflow server to JADEPUFFER, the AI-agent-driven operator it first documented earlier this month.

FakeGit campaign uses 7,600 GitHub repos to push SmartLoader malware

BleepingComputer - 21 July 2026 19:34

A large-scale operation dubbed 'FakeGit' is pushing SmartLoader and StealC malware through 7,600 malicious GitHub repositories that accumulated more than 14 million downloads.

Hacker Turns AI Jailbreaks Into Offensive Attack Platform

darkreading - 21 July 2026 19:38

A Russian-speaking actor, "Trim," dismantled publicly available frontier models and integrated them with offensive security tools.

Scottish Cyber Coordination Centre

Researchers Uncover North Korean 'ClickFake' Campaign Targeting Web3 Pros

Infosecurity Magazine - 21 July 2026 10:30

In a new campaign, North Korean hacking group Famous Chollima targeted crypto professionals through ClickFix lures to deliver Windows and macOS trojans.

Police dismantle Kratos phishing platform, arrest developer

BleepingComputer - 21 July 2026 20:07

Authorities in Germany and the U.S. dismantled the central infrastructure of Kratos, a phishing-as-a-service (PhaaS) platform with global reach, and its developer was arrested in Indonesia.