Scottish Cyber Coordination Centre

Daily Threat Bulletin

10 July 2026

Vulnerabilities

Microsoft fixed Defender flaw RoguePlanet (CVE-2026-50656)

Security Affairs - 09 July 2026 11:17

Microsoft fixed RoguePlanet (CVE-2026-50656), a Defender flaw allowing local attackers to gain higher privileges through the Malware Protection Engine.

CC-4810 - Microsoft SharePoint Remote Code Execution Vulnerability CVE-2026-33112

NHS Digital - 09 July 2026 11:59

Severity: Medium Successful exploitation of CVE-2026-33112 could allow an authorised attacker to achieve remote code execution on SharePoint servers via authenticated network access Successful exploitation of CVE-2026-33112 could allow an authorised attacker to achieve remote code execution on SharePoint servers via authenticated network access.

GhostApproval Symlink Flaws Could Let Malicious Repos Run Code in AI Coding Agents

The Hacker News - 09 July 2026 10:57

Researchers at Wiz found that a flaw in six popular AI coding assistants lets a booby-trapped code project quietly take control of a developer's computer. The assistant asks permission to edit one harmless-looking file, but the write lands on a sensitive one instead.

Palo Alto Networks Patches 13 Vulnerabilities

SecurityWeek - 09 July 2026 14:49

Buffer overflow, DoS, command injection, SSRF, authentication bypass, and other types of vulnerabilities have been found in PAN-OS software.

Chrome 150 Update Patches 27 Vulnerabilities

SecurityWeek - 09 July 2026 08:27

The security refresh resolves 13 use-after-free bugs, including two critical-severity flaws found by Google.

Microsoft expects more Windows security updates from AI-discovered flaws

BleepingComputer - 09 July 2026 14:00

Microsoft says Windows users should expect to see an increase in security updates as the company increasingly relies on artificial intelligence to discover vulnerabilities in its codebase.

Scottish Cyber Coordination Centre

Threat actors and malware

GodDamn Ransomware Uses PoisonX to Blind Security Software

Security Affairs - 09 July 2026 19:11

Symantec's Threat Hunter Team found a new ransomware family called GodDamn that first appeared in the wild on May 21, 2026, and analyzed an attack that took place in early June.

New GigaWiper Windows Backdoor Bundles Disk Wiping, Fake Ransomware, and Spyware

The Hacker News - 10 July 2026 00:38

Microsoft has taken apart a destructive Windows backdoor it calls GigaWiper. What stands out is how it is built: not one tool but three older destructive programs bolted into one, offered as commands the operator can choose from.

Vibe-Coded Malware Caught in Active Directory Attack

Infosecurity Magazine - 09 July 2026 15:00

Huntress found a threat actor using vibe-coded PowerShell to map an Active Directory network.

UK incidents

UK Government Rolls Out Agentic AI Defense Plan Alongside Industry Pledge

SecurityWeek - 09 July 2026 15:19

Two announcements on July 7, 2026, demonstrate the government's determination to improve the level of cybersecurity within the UK.