Scottish Cyber Coordination Centre

Daily Threat Bulletin

27 May 2026

Vulnerabilities

KnowledgeDeliver flaw exploited as a zero-day to install web shells

BleepingComputer - 26 May 2026 17:07

Hackers exploited a critical zero-day vulnerability in a server running the KnowledgeDeliver learning management system (LMS) to deploy the Godzilla web shell.

Microsoft Patches SharePoint RCE Flaw CVE-2026-45659 Across Server Versions

The Hacker News - 26 May 2026 18:19

Microsoft has rolled out updates to fix a remote code execution vulnerability impacting SharePoint that could be exploited by bad actors in attacks without requiring any specialized conditions to be met.

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-2026-48172 LiteSpeed cPanel Plugin Privilege Escalation Vulnerability

CC-4789 - Trend Micro Releases Security Update for Actively Exploited Medium Severity Vulnerability in Apex One

NHS Digital - 26 May 2026 13:36

Severity: Medium CVE-2026-34926 allows code injection via directory traversal in Trend Micro Apex One on-premise servers.

Threat actors and malware

Microsoft Defender can now automatically isolate hacked endpoints

BleepingComputer - 26 May 2026 09:19

Microsoft is testing a new Defender for Endpoint capability that will automatically isolate compromised endpoints to thwart attackers' attempts to move laterally across the network.

Scottish Cyber Coordination Centre

MuddyWater Uses DLL Side-Loading in Espionage Campaign Targeting 9 Countries

The Hacker News - 26 May 2026 22:18

The Iranian hacking group known as MuddyWater has been linked to a new campaign affecting at least nine organizations across nine countries on four continents in the first quarter of 2026.

Iranian Hackers Deploy MiniFast and MiniJunk V2 via Phishing and SEO Poisoning

The Hacker News - 26 May 2026 13:43

The Iranian state-sponsored threat actor known as Nimbus Manticore (aka Screening Serpens and UNC1549) has been attributed to a fresh campaign using lures impersonating organizations in the aviation and software sectors across the U.S., Europe, and the Middle East following the joint U.S.-Israeli military campaign against the country in late February 2026.