Scottish Cyber Coordination Centre

Daily Threat Bulletin

30 June 2026

Vulnerabilities

CC-4803 - Exploited Critical Vulnerability in the Oracle Payments Component of Oracle E-Business Suite

NHS Digital - 29 June 2026 16:26

Severity: High CVE-2026-46817 could allow unauthenticated remote takeover of Oracle Payments CVE-2026-46817 could allow unauthenticated remote takeover of Oracle Payments Updated: 29 Jun 2026

Amazon Q VS Extension Flaw Leads to Cloud Credential Theft

darkreading - 29 June 2026 12:44

Adversaries could plant a malicious repository that can execute arbitrary code and steal cloud credentials by exploiting the vulnerability, which showcases growing MCP risk.

'DirtyClone' Linux Kernel Vulnerability Leads to Root Access

SecurityWeek - 29 June 2026 12:20

A variant of DirtyFrag, the flaw allows unprivileged local users to manipulate the Linux page cache and gain root privileges.

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-2026-48558 SimpleHelp Authentication Bypass Vulnerability.

Threat actors and malware

Nissan discloses employee data breach linked to Oracle zero-day attacks

BleepingComputer - 29 June 2026 17:40

Nissan is warning that it suffered a data breach affecting current and former employees after threat actors exploited an Oracle PeopleSoft vulnerability in data theft attacks previously linked to the ShinyHunters extortion group. [...]

Hackers now exploit critical Oracle E-Business flaw in attacks

BleepingComputer - 29 June 2026 10:46

Scottish Cyber Coordination Centre

Attackers have begun exploiting a critical vulnerability (CVE-2026-46817) in the Oracle E-Business Suite (EBS) financial application, according to threat intelligence company Defused. [...]

Gamaredon Expands Ukraine Attacks with New Malware and Cloud Service Abuse

The Hacker News - 29 June 2026 18:10

A Russian advanced persistent threat (APT) group has continued to evolve and expand its malware arsenal as part of its ongoing cyber onslaught against Ukraine throughout 2025.

Microsoft Removes 119 Edge Extensions That Hid Malware in Images and Fonts

The Hacker News - 29 June 2026 15:02

Microsoft has shut down a long-running malicious extension operation on the Edge Add-ons store that hid its payloads inside ordinary image and font files, then woke up days after install to steal credentials and run ad fraud.

'Djinn' Stealer Targets Cloud, AI Credentials

darkreading - 29 June 2026 22:29

The infostealer was delivered via CVE-2026-48558, a critical authentication bypass vulnerability in SimpleHelp, targeting credentials linking development and admin environments to wider enterprise systems.

Iran, Russia, China Target Water Systems for Sabotage

darkreading - 29 June 2026 20:12

Nation-state attackers breach water systems through weak passwords, exposed PLCs, and poor segmentation — not sophisticated malware.

Russian Hackers Accused of Destructive Cyber-Attack on Jaguar Land Rover

Infosecurity Magazine - 29 June 2026 10:15

Experts warn the Jaguar Land Rover breach bears hallmarks of Kremlin-backed hackers, citing novel ransomware, strategic timing and efforts to obscure attribution