Scottish Cyber Coordination Centre

Daily Threat Bulletin

3 June 2026

Vulnerabilities

Oracle WebLogic CVE-2024-21182 Added to KEV Catalog After Active Exploitation

The Hacker News - 03 June 2026 00:44

The U.S. Cybersecurity and Infrastructure Security Agency (CISA) on Monday added a high-severity security flaw impacting Oracle WebLogic Server to its Known Exploited Vulnerabilities (KEV) Catalog, based on evidence of active exploitation.The vulnerability, CVE-2024-21182 (CVSS score: 7.5), allows an unauthenticated attacker with network access to take control of susceptible servers.

Critical Kirki flaw exploited to hijack WordPress admin accounts

BleepingComputer - 02 June 2026 19:12

Hackers are exploiting a critical privilege escalation vulnerability (CVE-2026-8206) in the Kirki plugin for WordPress to take over any user account, including those belonging to administrators.

CISA Adds Two Known Exploited Vulnerabilities to Catalog

CISA Advisories -

CISA has added two new vulnerabilities to its Known Exploited Vulnerabilities (KEV) Catalog, based on evidence of active exploitation.
CVE-2022-0492 Linux Kernel Improper Authentication Vulnerability
CVE-2025-48595 Android Framework Integer Overflow Vulnerability

Google June 2026 Android Update Patches 124 Flaws, One Actively Exploited

The Hacker News - 03 June 2026 01:16

Google on Monday released patches for 124 security vulnerabilities impacting its Android operating system for the month of June 2026, including one high-severity flaw in the Framework component that has come under active exploitation.

Android Update Patches Exploited Zero-Day, 123 Other Vulnerabilities

SecurityWeek - 02 June 2026 15:36

Google says the Android vulnerability CVE-2025-48595 has been exploited in limited, targeted attacks.

Scottish Cyber Coordination Centre

Threat actors and malware

AI-built ransomware toolkit automates EDR evasion, AD discovery

BleepingComputer - 02 June 2026 17:01

A threat actor is using an AI-built ransomware attack toolkit that automates Active Directory discovery and helps evade endpoint detection and response (EDR) solutions.

FBI-Flagged Phishing Kit Kali365 Expands Its Reach

darkreading - 02 June 2026 22:32

Once targeting just Microsoft 365, the phishing-as-a-service platform now aims at AWS, Okta, and Russian platforms, while relying on device code phishing.

Supply Chain Attack Hits 32 Red Hat NPM Packages

SecurityWeek - 02 June 2026 10:51

Hackers published 96 malicious package versions, injected with a credential-stealing worm similar to Mini Shai-Hulud.