Scottish Cyber Coordination Centre

Daily Threat Bulletin

12 June 2026

Vulnerabilities

Oracle mitigates PeopleSoft zero-day exploited in data theft attacks

BleepingComputer - 11 June 2026 16:39

Oracle is warning about a critical PeopleSoft Suite zero-day vulnerability tracked as CVE-2026-35273 that allows unauthenticated remote code execution, with the flaw actively exploited in ShinyHunter data theft attacks.

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-2026-10520 Ivanti Sentry OS Command Injection Vulnerability

CVE-2026-10520 Exploited: Ivanti Sentry Gateways Compromised Shortly After Patch Release

Security Affairs - 11 June 2026 18:57

Threat actors have started exploiting a maximum-severity OS command injection flaw in Ivanti Sentry, tracked as CVE-2026-10520, that allows remote code execution with root privileges.

New GreatXML Exploit Bypasses Windows BitLocker via Recovery Partition XML Files

The Hacker News - 12 June 2026 00:13

Security researcher Chaotic Eclipse (aka Nightmare-Eclipse and MSNightmare) has released a new Windows BitLocker bypass dubbed GreatXML, a day after they published an exploit for Microsoft Defender.

Fortinet patched a new critical FortiSandbox flaw

Security Affairs - 11 June 2026 10:51

Fortinet released security updates to address several vulnerabilities affecting FortiSandbox, FortiOS, FortiProxy, and FortiPortal. The most severe issue, tracked as CVE-2026-25089 (CVSS score of 9.8), is an OS command injection flaw in FortiSandbox products.

Splunk, Palo Alto Networks Patch Severe Vulnerabilities

SecurityWeek - 11 June 2026 11:47

The security defects could allow attackers to create or modify arbitrary files and access and modify protected resources.

Scottish Cyber Coordination Centre

Threat actors and malware

OnyxC2 Malware-as-a-Service Offers Enterprise-Grade Data Theft

Security Affairs - 11 June 2026 15:22

OnyxC2 is a MaaS stealer targeting 210+ apps, using DLL sideloading, encrypted payloads, and remote access features to evade detection.

Cybercriminals Use Fake AI Guides and Dev Tools to Spread AsyncRAT Malware

Infosecurity Magazine - 11 June 2026 15:00

Fake AI guides hide a multi-stage chain that drops AsyncRAT, with signs of AI-assisted coding.

New Attacks Trick OpenClaw AI Agent Into Running Code and Leaking Secrets

The Hacker News - 12 June 2026 00:16

Two security teams have shown, in separate research published this week, that OpenClaw, the popular self-hosted AI agent, can be driven to run attacker-controlled code or hand over sensitive data through ordinary-looking inputs.

The Gentlemen Ransomware Claims 478 Victims, Can Spread Like a Worm

The Hacker News - 11 June 2026 23:20

A new analysis of The Gentlemen operation has revealed that the financially motivated threat group initially operated as an affiliate responsible for conducting double extortion attacks, while leveraging resources from various ransomware-as-a-service (RaaS) schemes.

JDY Botnet Evolves After KV Takedown, Targets Military Networks

Security Affairs - 11 June 2026 08:46

Lumen's Black Lotus Labs reported the resurgence of the JDY botnet, a covert reconnaissance network tied to Chinese state-sponsored hacking groups including Volt Typhoon.

UK incidents

British high school sends students home following cyberattack

The Record from Recorded Future News - 11 June 2026 16:25

The majority of students at a high school in Buckinghamshire, England, were sent home for the second day in a row on Thursday after what the headteacher told parents was "a cybersecurity incident affecting our ICT systems."

University of Nottingham Confirms Breach After Hackers Leak Data

SecurityWeek - 11 June 2026 09:30

The ShinyHunters hacker group has taken credit for the attack, leaking more than 450,000 email addresses and other information.