Scottish Cyber Coordination Centre

Daily Threat Bulletin

11 June 2025

Vulnerabilities

New Secure Boot flaw lets attackers install bootkit malware, patch now

BleepingComputer - 10 June 2025 17:02

Security researchers have disclosed a new Secure Boot bypass tracked as CVE-2025-3052 that can be used to turn off security on PCs and servers and install bootkit malware.

Ivanti Workspace Control hardcoded key flaws expose SQL credentials

BleepingComputer - 10 June 2025 12:22

Ivanti has released security updates to fix three high-severity hardcoded key vulnerabilities in the company's Workspace Control (IWC) solution.

Microsoft warns of 66 flaws to fix for this Patch Tuesday, and two are under active attack

The Register - 11 June 2025 00:38

It's Patch Tuesday time again, and Microsoft is warning that there are a bunch of critical fixes to sort out - and two actively exploited bugs.

SAP June 2025 Security Patch Day fixed critical NetWeaver bug

Security Affairs - 10 June 2025 18:31

SAP June 2025 Security Patch addressed a critical NetWeaver vulnerability, tracked as CVE-2025-42989 (CVSS score of 9.6), allowing threat actors to bypass authorization checks and escalate their privileges.

Adobe Releases Patch Fixing 254 Vulnerabilities, Closing High-Severity Security Gaps

The Hacker News - 11 June 2025 00:59

Adobe on Tuesday pushed security updates to address a total of 254 security flaws impacting its software products, a majority of which affect Experience Manager (AEM).

Researchers Uncover 20+ Configuration Risks, Including Five CVEs, in Salesforce Industry Cloud

The Hacker News - 11 June 2025 00:34

Cybersecurity researchers have uncovered over 20 configuration-related risks affecting Salesforce Industry Cloud (aka Salesforce Industries), exposing sensitive data to unauthorized internal and external parties.

Scottish Cyber Coordination Centre

Threat actors and malware

FIN6 Uses AWS-Hosted Fake Resumes on LinkedIn to Deliver More_eggs Malware

The Hacker News - 10 June 2025 23:16

The financially motivated threat actor known as FIN6 has been observed leveraging fake resumes hosted on Amazon Web Services (AWS) infrastructure to deliver a malware family called More_eggs.

DanaBot malware operators exposed via C2 bug added in 2022

BleepingComputer - 10 June 2025 18:46

A vulnerability in the DanaBot malware operation introduced in June 2022 update led to the identification, indictment, and dismantling of their operations in a recent law enforcement action.

China-linked threat actor targeted +70 orgs worldwide, SentinelOne warns

Security Affairs - 10 June 2025 08:00

China-linked threat actor targeted over 70 global organizations, including governments and media, in cyber-espionage attacks from July 2024 to March 2025.

Rust-based Myth Stealer Malware Spread via Fake Gaming Sites Targets Chrome, Firefox Users

The Hacker News - 10 June 2025 20:50

Cybersecurity researchers have shed light on a previously undocumented Rust-based information stealer called Myth Stealer that's being propagated via fraudulent gaming websites.

Cloud brute-force attack cracks Google users' phone numbers in minutes

The Register - 10 June 2025 13:15

A researcher has exposed a flaw in Google's authentication systems, opening it to a brute-force attack that left users' mobile numbers up for grabs.

DDoS Attacks on Financial Sector Surge in Scale and Sophistication

Infosecurity Magazine - 10 June 2025 13:35

The financial sector was the industry most targeted by distributed denial-of-service (DDoS) attacks in 2024, with a peak in October.