Scottish Cyber Coordination Centre

Daily Threat Bulletin

2 October 2025

Vulnerabilities

OpenSSL patches 3 vulnerabilities, urging immediate updates

Security Affairs - 01 October 2025 21:15

The OpenSSL Project has released security updates to address three vulnerabilities, tracked as CVE-2025-9230, CVE-2025-9231, and CVE-2025-9232, in its open-source SSL/TLS toolkit.

Apple urges users to update iPhone and Mac to patch font bug

Security Affairs - 01 October 2025 12:00

Apple released iOS and macOS updates to address a medium-severity flaw, tracked as CVE-2025-43400, in font processing that could trigger a denial-of-service condition or memory corruption.

Adobe Analytics bug leaked customer tracking data to other tenants

BleepingComputer - 01 October 2025 16:58

Adobe is warning its Analytics customers that an ingestion bug caused data from some organizations to appear in the analytics instances of others for approximately one day.

New bug in classic Outlook can only be fixed via Microsoft support

BleepingComputer - 01 October 2025 15:43

Microsoft is investigating a known issue that causes the classic Outlook email client to crash upon launch, which can only be resolved via Exchange Online support.

Red Hat OpenShift AI Flaw Exposes Hybrid Cloud Infrastructure to Full Takeover

The Hacker News - 01 October 2025 19:06

A severe security flaw has been disclosed in the Red Hat OpenShift AI service that could allow attackers to escalate privileges and take control of the complete infrastructure under certain conditions.

OneLogin Bug Let Attackers Use API Keys to Steal OIDC Secrets and Impersonate Apps

The Hacker News - 01 October 2025 19:57

A high-severity security flaw has been disclosed in the One Identity, OneLogin, Identity and Access Management (IAM) solution that, if successfully exploited, could expose sensitive OpenID Connect (OIDC) application client secrets under certain circumstances.

Threat actors and malware

Google Sheds Light on ShinyHunters’ Salesforce Tactics

darkreading - 01 October 2025 22:17

Mandiant provided proactive defenses against UNC6040’s social engineering attacks that have led to several Salesforce breaches.

Android malware uses VNC to give attackers hands-on access

BleepingComputer - 01 October 2025 15:33

A new Android banking and remote access trojan (RAT) dubbed Klopatra disguised as an IPTV and VPN app has infected more than 3,000 devices across Europe.

NIST Publishes Guide for Protecting ICS Against USB-Borne Threats

SecurityWeek - 01 October 2025 12:16

NIST Special Publication 1334 focuses on reducing cybersecurity risks associated with the use of removable media devices in OT environments.