Scottish
Cyber
Coordination
Centre

Daily Threat Bulletin

16 June 2025

Vulnerabilities

Over 46,000 Grafana instances exposed to account takeover bug

BleepingComputer - 15 June 2025 11:07

More than 46,000 internet-facing Grafana instances remain unpatched and exposed to a client-side open redirect vulnerability that allows executing a malicious plugin and account takeover. [...]

Palo Alto Networks fixed multiple privilege escalation flaws

Security Affairs - 14 June 2025 10:56

Palo Alto Networks addressed multiple vulnerabilities and included the latest Chrome patches in its solutions. Palo Alto Networks fixed seven privilege escalation vulnerabilities and integrated the latest Chrome security patches into its products. Palo Alto applied 11 Chrome fixes and patched CVE-2025-4233, a cache vulnerability impacting the Prisma Access Browser.

Apple confirmed that Messages app flaw was actively exploited in the wild

Security Affairs - 13 June 2025 11:15

Apple confirmed that a security flaw in its Messages app was actively exploited in the wild to target journalists with Paragon’s Graphite spyware. Apple confirmed that a now-patched vulnerability, tracked as CVE-2025-43200, in its Messages app was actively exploited in the wild to target journalists with Paragon’s Graphite spyware.

Trend Micro fixes critical bugs in Apex Central and TMEE PolicyServer

Security Affairs - 13 June 2025 08:06

Trend Micro fixed multiple vulnerabilities that impact its Apex Central and Endpoint Encryption (TMEE) PolicyServer products. Trend Micro address remote code execution and authentication bypass vulnerabilities impacting its Endpoint Encryption (TMEE) PolicyServer and Apex Central solutions.

SimpleHelp Vulnerability Exploited Against Utility Billing Software Users

SecurityWeek - 13 June 2025 11:37

CISA warns that vulnerable SimpleHelp RMM instances have been exploited against a utility billing software provider’s customers.

Critical Vulnerability Exposes Many Mitel MiCollab Instances to Remote Hacking

SecurityWeek - 13 June 2025 09:29

Mitel has announced patches for a MiCollab path traversal vulnerability that can be exploited remotely without authentication.

Threat actors and malware

Anubis ransomware adds wiper to destroy files beyond recovery

BleepingComputer - 14 June 2025 11:29

<The Anubis ransomware-as-a-service (RaaS) operation has added to its file-encrypting malware a wiper module that destroys targeted files, making recovery impossible even if the ransom is paid. [...]

Discord flaw lets hackers reuse expired invites in malware campaign

BleepingComputer - 13 June 2025 13:10

Hackers are hijacking expired or deleted Discord invite links to redirect users to malicious sites that deliver remote access trojans and information-stealing malware. [...]

Unusual toolset used in recent Fog Ransomware attack

Security Affairs - 14 June 2025 07:38

Fog ransomware operators used in a May 2025 attack unusual pentesting and monitoring tools, Symantec researchers warn.

Over 269,000 Websites Infected with JSFireTruck JavaScript Malware in One Month

The Hacker News - 13 June 2025 20:42

Cybersecurity researchers are calling attention to a “large-scale campaign” that has been observed compromising legitimate websites with malicious JavaScript injections.

CISA Reveals ‘Pattern’ of Ransomware Attacks Against SimpleHelp RMM

darkreading - 13 June 2025 21:06

A new Cybersecurity and Infrastructure Security Agency (CISA) advisory warned ransomware actors have been actively exploiting a critical SimpleHelp flaw since January.

UK related

Introducing Guernsey Cyber Security Centre

Security Boulevard - 15 June 2025 17:45

In creating Guernsey Cyber Security Centre, JCSC are working with theStates of Guernsey to ensure all the Channel Islands have access tospecialist support for cyber security incidents, as well as advice andguidance to built better and more effective defences.The post Introducing Guernsey Cyber Security Centre appeared first on Security Boulevard.