Scottish Cyber Coordination Centre

Daily Threat Bulletin

17 June 2025

Vulnerabilities

ASUS Armoury Crate bug lets attackers get Windows admin privileges

BleepingComputer - 16 June 2025 15:08

A high-severity vulnerability in ASUS Armoury Crate software could allow threat actors to escalate their privileges to SYSTEM level on Windows machines. [...]

PyPI, npm, and AI Tools Exploited in Malware Surge Targeting DevOps and Cloud Environments

The Hacker News - 16 June 2025 13:15

Cybersecurity researchers from SafeDep and Veracode detailed a number of malware-laced npm packages that are designed to execute remote code and download additional payloads.

High-Severity Vulnerabilities Patched in Tenable Nessus Agent

SecurityWeek - 16 June 2025 09:53

Three high-severity Tenable Agent vulnerabilities could allow users to overwrite and delete files, or execute arbitrary code, with System privileges.

Over a Third of Grafana Instances Exposed to XSS Flaw

Infosecurity Magazine - 16 June 2025 10:15

Some 36% of Grafana instances are vulnerable to account takeover bug, putting DevOps teams at risk

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-2025-43200 Apple Multiple Products Unspecified Vulnerability, CVE-2023-33538 TP-Link Multiple Routers Command Injection Vulnerability.

Threat actors and malware

Hackers switch to targeting U.S. insurance companies

BleepingComputer - 16 June 2025 17:43

Threat intelligence researchers are warning of hackers breaching multiple U.S. companies in the insurance industry using all the tactics observed with Scattered Spider activity. [...]

Scottish Cyber Coordination Centre

Anubis Ransomware Encrypts and Wipes Files, Making Recovery Impossible Even After Payment

The Hacker News - 16 June 2025 20:51

An emerging ransomware strain has been discovered incorporating capabilities to encrypt files as well as permanently erase them, a development that has been described as a “rare dual-threat.

‘Water Curse’ Targets Infosec Pros via Poisoned GitHub Repositories

darkreading - 16 June 2025 17:45

The emerging threat group attacks the supply chain via weaponized repositories posing as legitimate pen-testing suites and other tools that are poisoned with malware.

Threat Actors Target Victims with HijackLoader and DeerStealer

Infosecurity Magazine - 16 June 2025 16:45

Cyber-attacks using HijackLoader and DeerStealer have been identified exploiting phishing tactics via ClickFix