Scottish Cyber Coordination Centre

Daily threat bulletin

7 August 2024

Vulnerabilities

Google Patches New Android Kernel Vulnerability Exploited in the Wild

The Hacker News - 06 August 2024 12:42

Google has addressed a high-severity security flaw impacting the Android kernel that it said has been actively exploited in the wild.The vulnerability, tracked as CVE-2024-36971, has been described as a case of remote code execution impacting the kernel."There are indications that CVE-2024-36971 may be under limited, targeted exploitation," the tech giant noted in its monthly Android security

Novel Threat Tactics, Notable Vulnerabilities, and Current Trends for June 2024

Security Boulevard - 06 August 2024 21:03

Every month, the Pondurance team hosts a webinar to keep clients current on the state of cybersecurity. In June, the team discussed threat intelligence, notable vulnerabilities and trends, threat hunting, security operations center (SOC) engineering insights, and deception technologies. Threat Intelligence The Assistant Vice President of Digital Forensics and Incident Response discussed Juneâ€™s heavy threat...The post Novel Threat Tactics, Notable Vulnerabilities, and Current Trends for June 2024 appeared first on Pondurance.The post Novel Threat Tactics, Notable Vulnerabilities, and Current Trends for June 2024 appeared first on Security Boulevard.

Threat actors and malware

Hacker wipes 13,000 devices after breaching classroom management platform

BleepingComputer - 06 August 2024 11:15

A hacker has breached Mobile Guardian, a digital classroom management platform used worldwide, and remotely wiped data from at least 13,000 student's iPads and Chromebooks. [...]

Attackers Use Multiple Techniques to Bypass Reputation-Based Security

darkreading - 06 August 2024 21:58

Protections like Windows Smart App Control are useful but susceptible to attacks that allow threat actors initial access to an environment without triggering any alerts.

Fighting Back Against Multi-Staged Ransomware Attacks Crippling Businesses

SecurityWeek - 06 August 2024 14:24

Scottish Cyber Coordination Centre

Modern ransomware attacks are multi-staged and highly targeted. First, attackers research the target organization and its employees.The post Fighting Back Against Multi-Staged Ransomware Attacks Crippling Businesses appeared first on SecurityWeek.

CrowdStrike Releases Root Cause Analysis of Falcon Sensor BSOD Crash

SecurityWeek - 06 August 2024 21:51

Embattled cybersecurity vendor CrowdStrike on Tuesday released a root cause analysis detailing the technical mishap behind a software update crash that crippled Windows systems globally and blamed the incident on a confluence of security vulnerabilities and process gaps.

UK related

NHS software supplier Advanced faces £6m fine over ransomware attack failings

The Record from Recorded Future News - 07 August 2024 01:55