Scottish Cyber Coordination Centre

Daily Threat Bulletin

13 June 2024

Vulnerabilities

Google warns of actively exploited Pixel firmware zero-day

BleepingComputer - 12 June 2024 16:06

Google has released patches for 50 security vulnerabilities impacting its Pixel devices and warned that one of them had already been exploited in targeted attacks as a zero-day.

Black Basta Ransomware May Have Exploited MS Windows Zero-Day Flaw

The Hacker News - 12 June 2024 17:41

Threat actors linked to the Black Basta ransomware may have exploited a recently disclosed privilege escalation flaw in the Microsoft Windows Error Reporting Service as a zero-day, according to new findings from Symantec. The security flaw in question is CVE-2024-26169 (CVSS score: 7.8), an elevation of privilege bug in the Windows Error Reporting Service.

Scores of Biometrics Bugs Emerge, Highlighting Authentication Risks

darkreading - 12 June 2024 21:41

Face scans stored like passwords inevitably will be compromised, like passwords are. But there's a crucial difference between the two that organisations can rely on when their manufacturers fail.

TellYouthePass Ransomware Group Exploits Critical PHP Flaw

darkreading - 12 June 2024 16:41

An RCE vulnerability that affects the Web scripting language on Windows systems is easy to exploit and can provide a broad attack surface.

UEFI Firmware Exploit Evades EDR

Security Boulevard - 12 June 2024 23:43

As endpoint security tools improve, attackers target lower level firmware components to evade detection. This demo shows how malware targeting UEFI firmware, such as Black Lotus, can evade Windows device security features and EDR Vendor 1, and give attackers stealthy and persistent access to systems.

Fortinet Patches Code Execution Vulnerability in FortiOS

SecurityWeek - 12 June 2024 13:45

Fortinet has patched multiple vulnerabilities in FortiOS, including a high-severity code execution security flaw.

Scottish Cyber Coordination Centre

Threat actors and malware

New Cross-Platform Malware 'Noodle RAT' Targets Windows and Linux Systems

The Hacker News - 13 June 2024 12:55

A previously undocumented cross-platform malware codenamed Noodle RAT has been put to use by Chinese-speaking threat actors either for espionage or cybercrime for years. While this backdoor was previously categorized as a variant of Gh0st RAT and Rekoobe, Trend Micro security researcher Hara Hiroaki said "this backdoor is not merely a variant of existing malware, but is a new type altogether."

Research reveals new ransomware variant called Fog

Security Magazine - 12 June 2024 09:00

Research has revealed the development of a new ransomware variant called Fog. The research, conducted by Arctic Wolf Labs, was observed in multiple cases and displayed similar elements throughout.

RansomHub Brings Scattered Spider Into Its RaaS Nest

darkreading - 12 June 2024 11:00

The threat group behind breaches at Caesars and MGM moves its business over to a different ransomware-as-a-service operation. The RansomHub RaaS group appears to have scored a major victory by attracting the Scattered Spider threat group into its affiliate ranks, according to new research from GuidePoint Security.

Self-replicating Morris II worm targets AI email assistants

Security Intelligence - 12 June 2024 14:00

The proliferation of generative artificial intelligence (GenAI) email assistants such as OpenAI, GPT-3 and Google’s Smart Compose has revolutionized communication workflows. Unfortunately, it has also introduced novel attack vectors for cyber criminals. Leveraging recent advancements in AI and natural language processing, malicious actors can exploit vulnerabilities in GenAI systems to orchestrate sophisticated cyberattacks.