Scottish Cyber Coordination Centre

Daily Threat Bulletin

16 August 2024

Vulnerabilities

GitHub Vulnerability 'ArtiPACKED' Exposes Repositories to Potential Takeover

The Hacker News - 15 August 2024 13:17

A newly discovered attack vector in GitHub Actions artifacts dubbed ArtiPACKED could be exploited to take over repositories and gain access to organizations' cloud environments.

SolarWinds: Critical RCE Bug Requires Urgent Patch

darkreading - 15 August 2024 19:51

The vulnerability was given a high-severity CVSS score, indicating that customers should act swiftly to mitigate the flaw.

Zero-Click Exploit Concerns Drive Urgent Patching of Windows TCP/IP Flaw

SecurityWeek - 15 August 2024 16:39

Security experts are ratcheting up the urgency for Windows admins to patch a wormable, pre-auth remote code execution vulnerability in the Windows TCP/IP stack.

Palo Alto Networks Patches Unauthenticated Command Execution Flaw in Cortex XSOAR

SecurityWeek - 15 August 2024 12:29

Palo Alto Networks has patched multiple vulnerabilities, including ones rated high severity, in several products.

Microsoft patches bug that could have allowed an attacker to revert your computer back to an older, vulnerable version

Malwarebytes - 15 August 2024 11:38

A researcher used two Windows vulnerabilities to perform downgrade attacks. These flaws have now been patched by Microsoft.

Google to remove app from Pixel devices following claims that it made phones vulnerable

The Record from Recorded Future News - 15 August 2024 21:10

Google and a cybersecurity company are disputing over claims that an application on Android phones left the devices vulnerable to cyberattacks and spyware.

Threat actors and malware

Ransomware gang deploys new malware to kill security software

BleepingComputer - 15 August 2024 15:01

RansomHub ransomware operators have been spotted deploying new malware to disable Endpoint Detection and Response (EDR) security software in Bring Your Own Vulnerable Driver (BYOVD) attacks.

Google disrupted hacking campaigns carried out by Iran-linked APT42

Security Affairs - 15 August 2024 18:30

Google announced that it disrupted a hacking campaign carried out by Iran-linked group APT42 (Calanque, UNC788) that targeted the personal email accounts of individuals associated with the US elections.

Black Basta ransomware gang linked to a SystemBC malware campaign

Security Affairs - 15 August 2024 09:40

Experts linked an ongoing social engineering campaign, aimed at deploying the malware SystemBC, to the Black Basta ransomware group. Rapid7 researchers uncovered a new social engineering campaign distributing the SystemBC dropper to the Black Basta ransomware operation.

Lessons from the Snowflake breach: SaaS security needs collaboration

Security Magazine - 15 August 2024 09:00

Companies should align their SaaS security strategies with their service providers so that everyone is clear on what role they should play in mitigating threats.