Scottish Cyber Coordination Centre

Daily Threat Bulletin

12 June 2024

Vulnerabilities

JetBrains warns of IntelliJ IDE bug exposing GitHub access tokens

BleepingComputer - 11 June 2024 15:59

JetBrains warned customers to patch a critical vulnerability that impacts users of its IntelliJ integrated development environment (IDE) apps and exposes GitHub access tokens.

Critical MSMQ RCE Bug Opens Microsoft Servers to Complete Takeover

darkreading - 12 June 2024 00:04

CVE-2024-30080 is the only critical issue in Microsoft's June 2024 Patch Tuesday update, but many others require prompt attention as well.

Apple Patches Vision Pro Vulnerability Used in Possibly 'First Ever Spatial Computing Hack'

SecurityWeek - 11 June 2024 14:38

Apple on Monday updated visionOS, the operating system powering its Vision Pro virtual reality headset, to version 1.2, which addresses several vulnerabilities, including what may be the first security flaw that is specific to the VR headset.

Threat actors and malware

Chinese hackers breached 20,000 FortiGate systems worldwide

BleepingComputer - 11 June 2024 13:22

The Dutch Military Intelligence and Security Service (MIVD) warned today that the impact of a Chinese cyber-espionage campaign unveiled earlier this year is "much larger than previously known."

Pure Storage confirms data breach after Snowflake account hack

BleepingComputer - 11 June 2024 09:48

Pure Storage, a leading provider of cloud storage systems and services, confirmed on Monday that attackers breached its Snowflake workspace and gained access to what the company describes as telemetry information.

Scottish Cyber Coordination Centre

Chinese Actor SecShow Conducts Massive DNS Probing on Global Scale

The Hacker News - 11 June 2024 21:02

Cybersecurity researchers have shed more light on a Chinese actor codenamed SecShow that has been observed conducting Domain Name System (DNS) on a global scale since at least June 2023.

China-Linked ValleyRAT Malware Resurfaces with Advanced Data Theft Tactics

The Hacker News - 11 June 2024 15:17

Cybersecurity researchers have uncovered an updated version of malware called ValleyRAT that's being distributed as part of a new campaign. In the latest version, ValleyRAT introduced new commands, such as capturing screenshots, process filtering, forced shutdown, and clearing Windows event logs.

WarmCookie Gives Cyberattackers Tasty New Backdoor for Initial Access

darkreading - 11 June 2024 17:26

The fresh-baked malware is being widely distributed, but still specifically targets individuals with tailored lures. It's poised to evolve into a bigger threat, researchers warn.

Threat Actor Breaches Snowflake Customers, Victims Extorted

Infosecurity Magazine - 11 June 2024 14:35

Mandiant warns that a financially-motivated threat actor stole a significant volume of customer data from Snowflake, and is extorting many of the victims