Scottish
Cyber
Coordination
Centre

Daily Threat Bulletin

14 June 2024

Vulnerabilities

Exploit for Veeam Recovery Orchestrator auth bypass available, patch now

BleepingComputer - 13 June 2024 14:21

A proof-of-concept (PoC) exploit for a critical Veeam Recovery Orchestrator authentication bypass vulnerability tracked as CVE-2024-29855 has been released, elevating the risk of being exploited in attacks.

PoC Exploit Emerges for Critical RCE Bug in Ivanti Endpoint Manager

darkreading - 13 June 2024 20:16

A new month, a new high-risk Ivanti bug for attackers to exploit — this time, an SQL injection issue in its centralized endpoint manager.

Microsoft, Late to the Game on Dangerous DNSSEC Zero-Day Flaw

darkreading - 13 June 2024 15:30

Why the company took so long to address the issue is not known given that most other stakeholders had a fix out for the issue months ago.

Kaspersky Finds 24 Flaws in Chinese Biometric Hardware Provider

Infosecurity Magazine - 13 June 2024 12:30

A series of vulnerabilities could enable an attacker to bypass the Chinese manufacturer's biometric access systems

Update now! Google Pixel vulnerability is under active exploitation

Malwarebytes - 13 June 2024 14:33

Google revealed that a firmware vulnerability in its Pixel devices has been under limited active exploitation

Scottish Cyber Coordination Centre

Threat actors and malware

Arid Viper Launches Mobile Espionage Campaign with AridSpy Malware

The Hacker News - 13 June 2024 20:25

The threat actor known as Arid Viper has been attributed to a mobile espionage campaign that leverages trojanized Android apps to deliver a spyware strain dubbed AridSpy. The malware is distributed through dedicated websites impersonating various messaging apps, a job opportunity app, and a Palestinian Civil Registry app.

Pakistan-linked Malware Campaign Evolves to Target Windows, Android, and macOS

The Hacker News - 13 June 2024 16:56

Threat actors with ties to Pakistan have been linked to a long-running malware campaign dubbed Operation Celestial Force since at least 2018. The activity, still ongoing, entails the use of an Android malware called GravityRAT and a Windows-based malware loader codenamed HeavyLift, according to Cisco Talos.

Cybercriminals Employ PhantomLoader to Distribute SSLoad Malware

The Hacker News - 13 June 2024 16:49

The nascent malware known as SSLoad is being delivered by means of a previously undocumented loader called PhantomLoader, according to findings from cybersecurity firm Intezer.

North Korea's Moonstone Sleet Widens Distribution of Malicious Code

darkreading - 13 June 2024 19:56

The recently identified threat actor uses public registries for distribution and has expanded capabilities to disrupt the software supply chain.

Intel 471 Sets New Standard in Intelligence-Driven Threat Hunting

Security Boulevard - 13 June 2024 19:25

Relentless ransomware, damaging malware, emerging cyber adversaries and rapidly advancing artificial intelligence (AI) have changed the threat landscape, particularly for critical infrastructure. In an effort to meet this growing need, Intel 471 has acquired Cyborg Security, the company behind HUNTER — a powerful threat hunting platform for proactively detecting stealthy threats.

A Deep Dive Into the Economics and Tactics of Modern Ransomware Threat Actors

Security Boulevard - 14 June 2024 07:08

The MGM Resorts breach is just one example demonstrating the crippling financial, legal and operational consequences of ransomware incidents. Recently, we have seen a fundamental shift in the strategies employed by highly coordinated threat actor groups like ALPHV/BlackCat and Scattered Spider who prioritize targeting infrastructure over endpoints during incident responses to bypass modern investments in cybersecurity solutions.