Scottish Cyber Coordination Centre

Daily threat bulletin

11 July 2024

Vulnerabilities

GitLab: Critical bug lets attackers run pipelines as other users

BleepingComputer - 10 July 2024 17:08

GitLab warned today that a critical vulnerability in its product's GitLab Community and Enterprise editions allows attackers to run pipeline jobs as any other user.

Windows MSHTML zero-day used in malware attacks for over a year

BleepingComputer - 10 July 2024 13:04

Microsoft fixed a Windows zero-day vulnerability that has been actively exploited in attacks for eighteen months to launch malicious scripts while bypassing built-in security features.

Citrix fixed critical and high-severity bugs in NetScaler product

Security Affairs - 10 July 2024 15:31

IT giant Citrix addressed multiple vulnerabilities, including critical and high-severity issues in its NetScaler product. Citrix released security updates to address critical and high-severity issues in its NetScaler product. The most severe issue is an improper authorization flaw, tracked as CVE-2024-6235 (CVSS score of 9.4).

PHP Vulnerability Exploited to Spread Malware and Launch DDoS Attacks

The Hacker News - 11 July 2024 11:49

Multiple threat actors have been observed exploiting a recently disclosed security flaw in PHP to deliver remote access trojans, cryptocurrency miners, and distributed denial-of-service (DDoS) botnets.The vulnerability in question is CVE-2024-4577 (CVSS score: 9.8), which allows an attacker to remotely execute malicious commands on Windows systems using Chinese and Japanese language locales.

VMware Patches Critical SQL-Injection Flaw in Aria Automation

SecurityWeek - 10 July 2024 17:23

VMware warns that authenticated malicious users could enter specially crafted SQL queries and perform unauthorized read/write operations in the database.

Microsoft Outlook Faced Critical Zero-Click RCE Vulnerability

Infosecurity Magazine - 10 July 2024 16:30

For trusted senders, the flaw is zero-click, but requires one-click interactions for untrusted ones

Scottish Cyber Coordination Centre

Threat actors and malware

Japan warns of attacks linked to North Korean Kimsuky hackers

BleepingComputer - 10 July 2024 14:10

Japan's Computer Emergency Response Team Coordination Center (JPCERT/CC) is warning that Japanese organizations are being targeted in attacks by the North Korean 'Kimsuky' threat actors.

New Ransomware Group Exploiting Veeam Backup Software Vulnerability

The Hacker News - 10 July 2024 19:36

A now-patched security flaw in Veeam Backup & Replication software is being exploited by a nascent ransomware operation known as EstateRansomware.Singapore-headquartered Group-IB, which discovered the threat actor in early April 2024, said the modus operandi involved the exploitation of CVE-2023-27532 (CVSS score: 7.5) to carry out the malicious activities.

Ransomware Groups Prioritize Defense Evasion for Data Exfiltration

Infosecurity Magazine - 10 July 2024 13:00

A Cisco report highlighted TTPs used by the most prominent ransomware groups to evade detection, establish persistence and exfiltrate sensitive data.

The Stark Truth Behind the Resurgence of Russia's Fin7

Krebs on Security - 10 July 2024 17:22

The Russia-based cybercrime group dubbed "Fin7," known for phishing and malware attacks that have cost victim organizations an estimated $3 billion in losses since 2013, was declared dead last year by U.S. authorities. But experts say Fin7 has roared back to life in 2024 – setting up thousands of websites mimicking a range of media and technology companies – with the help of Stark Industries Solutions, a sprawling hosting provider is a persistent source of cyberattacks against enemies of Russia.