Scottish
Cyber
Coordination
Centre

Daily threat bulletin

30 April 2024

Vulnerabilities

Microsoft fixes bug behind incorrect BitLocker encryption errors

BleepingComputer - 29 April 2024 12:04

Microsoft has fixed a known issue causing incorrect BitLocker drive encryption errors in some managed Windows environments. [...]

Sandbox Escape Vulnerabilities in Judge0 Expose Systems to Complete Takeover

The Hacker News - 29 April 2024 16:28

Multiple critical security flaws have been disclosed in the Judge0 open-source online code execution system that could be exploited to obtain code execution on the target system.The three flaws, all critical in nature, allow an “adversary with sufficient access to perform a sandbox escape and obtain root permissions on the host machine.”

R Programming Bug Exposes Orgs to Vast Supply Chain Risk

darkreading - 29 April 2024 21:51

The CVE-2024-27322 security vulnerability in R’s deserialization process gives attackers a way to execute arbitrary code in target environments via specially crafted files.

[R1] Nessus Network Monitor 6.4.0 Fixes Multiple Vulnerabilities

Tenable Product Security Advisories - 29 April 2024 16:40

Nessus Network Monitor 6.4.0 Fixes Multiple VulnerabilitiesArnie CabralMon, 04/29/2024 - 11:40 Nessus Network Monitor leverages third-party software to help provide underlying functionality. Several of the third-party components (hyperscan, curl and c-ares) were found to contain vulnerabilities, and updated versions have been made available by the providers.Out of caution and in line with best practice, Tenable has opted to upgrade these components to address the potential impact of the issues. Nessus Network Monitor 6.4.0 updates hyperscan to version 5.4.2, curl to version 8.6.0, and c-ares to version 1.28.0.

Threat actors and malware

China-Linked ‘Muddling Meerkat’ Hijacks DNS to Map Internet on Global Scale

The Hacker News - 29 April 2024 20:16

A previously undocumented cyber threat dubbed Muddling Meerkat has been observed undertaking sophisticated domain name system (DNS) activities in a likely effort to evade security measures and conduct reconnaissance of networks across the world since October 2019.

Okta: Credential-Stuffing Attacks Spike via Proxy Networks

darkreading - 29 April 2024 21:25

Okta warns users that the attack requests are made through an anonymizing service like Tor or various commercial proxy networks.

Honeywell: USB Malware Attacks on Industrial Orgs Becoming More Sophisticated

SecurityWeek - 29 April 2024 14:00

An analysis conducted by Honeywell shows that much of the USB-borne malware targeting industrial organizations can still cause OT disruption.The post Honeywell: USB Malware Attacks on Industrial Orgs Becoming More Sophisticated appeared first on SecurityWeek.