Scottish
Cyber
Coordination
Centre

Daily threat bulletin

17 October 2024

Vulnerabilities

Critical Kubernetes Image Builder flaw gives SSH root access to VMs

BleepingComputer - 16 October 2024 13:58

A critical vulnerability in Kubernetes could allow unauthorized SSH access to a virtual machine running an image created with the Kubernetes Image Builder project. [...]

VMware Patches High-Severity SQL Injection Flaw in HCX Platform

SecurityWeek - 16 October 2024 19:25

VMware patches CVE-2024-38814 and warns that attackers with non-administrator privileges can execute remote code on the HCX manager.

Microsoft Patches Vulnerabilities in Power Platform, Imagine Cup Site

SecurityWeek - 16 October 2024 13:27

Microsoft has patched ‘critical’ privilege escalation and information disclosure vulnerabilities in Power Platform, Dataverse and the Imagine Cup website.

Tor Browser and Firefox users should update to fix actively exploited vulnerability

Malwarebytes - 16 October 2024 12:37

Mozilla warns that a vulnerability in Firefox and Tor Browser is actively being exploited against both browsers.

Threat actors and malware

Iranian hackers act as brokers selling critical infrastructure access

BleepingComputer - 16 October 2024 20:16

Iranian hackers are breaching critical infrastructure organizations to collect credentials and network data that can be sold on cybercriminal forums to enable cyberattacks from other threat actors. [...]

North Korean ScarCruft Exploits Windows Zero-Day to Spread RokRAT Malware

The Hacker News - 16 October 2024 17:20

The North Korean threat actor known as ScarCruft has been linked to the zero-day exploitation of a now-patched security flaw in Windows to infect devices with malware known as RokRAT. The vulnerability in question is CVE-2024-38178 (CVSS score: 7.5), a memory corruption bug in the Scripting Engine that could result in remote code execution when using the Edge browser in Internet Explorer Mode.

Iran's APT34 Abuses MS Exchange to Spy on Gulf Gov'ts

darkreading - 17 October 2024 07:00

A MOIS-aligned threat group has been using Microsoft Exchange servers to exfiltrate sensitive data from Gulf-state government agencies.

Ethical Hackers Embrace AI Tools Amid Rising Cyber Threats

Infosecurity Magazine - 16 October 2024 16:15

A new Bugcrowd study shows 71% of ethical hackers now see AI boosting hacking value, up from 21% in 2023.