Scottish
Cyber
Coordination
Centre

Daily threat bulletin

1 October 2024

Vulnerabilities

Critical flaw in NVIDIA Container Toolkit allows full host takeover

BleepingComputer - 29 September 2024 11:23

A critical vulnerability in NVIDIA Container Toolkit impacts all AI applications in a cloud or on-premise environment that rely on it to access GPU resources. [...]

Progress Software fixed 2 new critical flaws in WhatsUp Gold

Security Affairs - 29 September 2024 08:43

Progress Software addresses six new security vulnerabilities affecting its WhatsUp Gold, two of them are rated as critical severity. Progress Software has addressed six new security vulnerabilities in its IT infrastructure monitoring product WhatsUp Gold.

Critical Linux CUPS Printing System Flaws Could Allow Remote Command Execution

The Hacker News - 27 September 2024 19:03

A new set of security vulnerabilities has been disclosed in the OpenPrinting Common Unix Printing System (CUPS) on Linux systems that could permit remote command execution under certain conditions.

Novel Exploit Chain Enables Windows UAC Bypass

darkreading - 27 September 2024 20:16

Adversaries can exploit CVE-2024-6769 to jump from regular to admin access without triggering UAC, but Microsoft says it’s not really a vulnerability.

CISA Adds Four Known Exploited Vulnerabilities to Catalog

CISA Advisories -

CISA has added four new vulnerabilities to its Known Exploited Vulnerabilities Catalog, based on evidence of active exploitation: CVE-2023-25280 D-Link DIR-820 Router OS Command Injection Vulnerability; CVE-2020-15415 DrayTek Multiple Vigor Routers OS Command Injection Vulnerability; CVE-2021-4043 Motion Spell GPAC Null Pointer Dereference Vulnerability; CVE-2019-0344 SAP Commerce Cloud Deserialization of Untrusted Data Vulnerability information.

Threat actors and malware

Microsoft Identifies Storm-0501 as Major Threat in Hybrid Cloud Ransomware Attacks

The Hacker News - 27 September 2024 17:41

The threat actor known as Storm-0501 has targeted government, manufacturing, transportation, and law enforcement sectors in the U.S. to stage ransomware attacks.

New Cryptojacking Attack Targets Docker API to Create Malicious Swarm Botnet

The Hacker News - 01 October 2024 11:42

Cybersecurity researchers have uncovered a new cryptojacking campaign targeting the Docker Engine API with the goal of co-opting the instances to join a malicious Docker Swarm controlled by the threat actor.

Magecart Attacks Surge as E-Commerce Security Struggles to Keep Pace

Security Boulevard - 30 September 2024 18:32

A new report by Recorded Future’s Insikt Group reveals a concerning rise in Magecart attacks and e-skimming activity targeting online retailers. The research highlights how cybercriminals are evolving their tactics to bypass traditional, rather antiquated client-side security measures such as Content Security Policy (CSP) and compromise e-commerce platforms at an alarming rate.

North Korea Hackers Linked to Breach of German Missile Manufacturer

SecurityWeek - 30 September 2024 18:19

The targeting of Diehl Defence is significant because the company specializes in the production of missiles and ammunition.

JPCERT shares Windows Event Log tips to detect ransomware attacks

BleepingComputer - 30 September 2024 16:22

Japan’s Computer Emergency Response Center (JPCERT/CC) has shared tips on detecting different ransomware gang’s attacks based on entries in Windows Event Logs, providing timely detection of ongoing attacks before they spread too far into a network. […]

Session Hijacking 2.0 — The Latest Way That Attackers are Bypassing MFA

The Hacker News - 30 September 2024 17:50

Attackers are increasingly turning to session hijacking to get around widespread MFA adoption. The data supports this, as:147,000 token replay attacks were detected by Microsoft in 2023, a 111% increase year-over-year (Microsoft).

UK related

British National Arrested, Charged for Hacking US Companies

SecurityWeek - 30 September 2024 10:02

UK national Robert Westbrook was charged in the US for executing a hack-to-trade scheme against five public companies.

Man Arrested Over UK Railway Station Wi-Fi Hack

Infosecurity Magazine - 27 September 2024 11:00

The suspect is an employee of Global Reach Technology, which provides some Wi-Fi services to Network Rail