Scottish Cyber Coordination Centre

Daily threat bulletin

12 December 2024

Vulnerabilities

Ivanti fixed a maximum severity vulnerability in its CSA solution

Security Affairs - 11 December 2024 15:47

Ivanti addressed a critical authentication bypass vulnerability impacting its Cloud Services Appliance (CSA) solution. Ivanti addressed a critical authentication bypass vulnerability, tracked as CVE-2024-11639 (CVSS score of 10), in its Cloud Services Appliance (CSA) solution.

Microsoft MFA AuthQuake Flaw Enabled Unlimited Brute-Force Attempts Without Alerts

The Hacker News - 11 December 2024 21:02

Cybersecurity researchers have flagged a “critical” security vulnerability in Microsoft’s multi-factor authentication (MFA) implementation that allows an attacker to trivially sidestep the protection and gain unauthorized access to a victim’s account.

Atlassian, Splunk Patch High-Severity Vulnerabilities

SecurityWeek - 11 December 2024 14:00

Atlassian and Splunk on Tuesday announced patches for over two dozen vulnerabilities, including high-severity flaws.

Hunk Companion WordPress plugin exploited to install vulnerable plugins

BleepingComputer - 11 December 2024 19:28

Hackers are exploiting a critical vulnerability in the “Hunk Companion” plugin to install and activate other plugins with exploitable flaws directly from the WordPress.org repository. [...]

Threat actors and malware

New Malware Technique Could Exploit Windows UI Framework to Evade EDR Tools

The Hacker News - 11 December 2024 21:43

A newly devised technique leverages a Windows accessibility framework called UI Automation (UIA) to perform a wide range of malicious activities without tipping off endpoint detection and response (EDR) solutions.

ZLoader Malware Returns With DNS Tunneling to Stealthily Mask C2 Comms

The Hacker News - 11 December 2024 20:37

Scottish Cyber Coordination Centre

Cybersecurity researchers have discovered a new version of the ZLoader malware that employs a Domain Name System (DNS) tunnel for command-and-control (C2) communications, indicating that the threat actors are continuing to refine the tool after resurfacing a year ago.

New EagleMsgSpy Android spyware used by Chinese police, researchers say

BleepingComputer - 11 December 2024 17:03

A previously undocumented Android spyware called 'EagleMsgSpy' has been discovered and is believed to be used by law enforcement agencies in China to monitor mobile devices. [...]

Secret Blizzard Deploys Kazuar Backdoor in Ukraine Using Amadey Malware-as-a-Service

The Hacker News - 12 December 2024 00:32

The Russian nation-state actor tracked as Secret Blizzard has been observed leveraging malware associated with other threat actors to deploy a known backdoor called Kazuar on target devices located in Ukraine.

BadRAM Attack Uses $10 Equipment to Break AMD Processor Protections

SecurityWeek - 11 December 2024 16:57

Academic researchers devise BadRAM, a new attack that uses $10 equipment to break AMD's latest trusted execution environment protections.

Europol Dismantles 27 DDoS Attack Platforms Across 15 Nations; Admins Arrested

The Hacker News - 12 December 2024 12:45

A global law enforcement operation has failed 27 stresser services that were used to conduct distributed denial-of-service (DDoS) attacks and took them offline as part of a multi-year international exercise called PowerOFF.