Scottish
Cyber
Coordination
Centre

Daily threat bulletin

14 August 2024

Vulnerabilities

New Windows SmartScreen bypass exploited as zero-day since March

BleepingComputer - 13 August 2024 19:43

Today, Microsoft revealed that a Mark of the Web security bypass vulnerability exploited by attackers as a zero-day to bypass SmartScreen protection was patched during the June 2024 Patch Tuesday. [...]

Critical SAP flaw allows remote attackers to bypass authentication

BleepingComputer - 13 August 2024 18:43

SAP has released its security patch package for August 2024, addressing 17 vulnerabilities, including a critical authentication bypass that could allow remote attackers to fully compromise the system. [...]

Microsoft Issues Patches for 90 Flaws, Including 10 Critical Zero-Day Exploits

The Hacker News - 14 August 2024 12:18

Microsoft on Tuesday shipped fixes to address a total of 90 security flaws, including 10 zero-days, of which six have come under active exploitation in the wild.Of the 90 bugs, seven are rated Critical, 79 are rated Important, and one is rated Moderate in severity. This is also in addition to 36 vulnerabilities that the tech giant resolved in its Edge browser since last month.

Critical Flaw in Ivanti Virtual Traffic Manager Could Allow Rogue Admin Access

The Hacker News - 14 August 2024 11:48

Ivanti has rolled out security updates for a critical flaw in Virtual Traffic Manager (vTM) that could be exploited to achieve an authentication bypass and create rogue administrative users. The vulnerability, tracked as CVE-2024-7593, has a CVSS score of 9.8 out of a maximum of 10.0.

Microsoft Azure AI Health Bot Infected With Critical Vulnerabilities

darkreading - 13 August 2024 19:36

Privilege escalation flaws in the healthcare chatbot platform could have allowed unauthorized cross-tenant access and management of other customers’ resources.

Adobe Calls Attention to Massive Batch of Code Execution Flaws

SecurityWeek - 13 August 2024 18:12

Patch Tuesday: Adobe patches 72 security vulnerabilities and warns that Windows and macOS users are at risk of code execution, memory leaks, and denial-of-service attacks. The post Adobe Calls Attention to Massive Batch of Code Execution Flaws appeared first on SecurityWeek.

CISA Adds Six Known Exploited Vulnerabilities to Catalog

CISA Advisories -

CISA has added six new vulnerabilities to its Known Exploited Vulnerabilities Catalog, based on evidence of active exploitation: CVE-2024-38189 Microsoft Project Remote Code Execution Vulnerability; CVE-2024-38178 Microsoft Windows Scripting Engine Memory Corruption Vulnerability; CVE-2024-38213 Microsoft Windows SmartScreen Security Feature Bypass Vulnerability; CVE-2024-38193 Microsoft Windows Ancillary Function Driver for WinSock Privilege Escalation Vulnerability; CVE-2024-38106 Microsoft Windows Kernel Privilege Escalation Vulnerability; CVE-2024-38107 Microsoft Windows Power Dependency Coordinator Privilege Escalation Vulnerability.

Threat actors and malware

China-Backed Earth Baku Expands Cyber Attacks to Europe, Middle East, and Africa

The Hacker News - 14 August 2024 11:31

The China-backed threat actor known as Earth Baku has diversified its targeting footprint beyond the Indo-Pacific region to include Europe, the Middle East, and Africa starting in late 2022. Newly targeted countries as part of the activity include Italy, Germany, the U.A.E., and Qatar, with suspected attacks also detected in Georgia and Romania.

Six ransomware gangs behind over 50% of 2024 attacks

The Register - 13 August 2024 21:00

Plus many more newbies waiting in the wings Despite a law enforcement takedown six months ago, LockBit 3.0 remains the most prolific encryption and extortion gang, at least so far, this year, according to Palo Alto Networks' Unit 42.

China-linked hackers could be behind cyberattacks on Russian state agencies, researchers say

The Record from Recorded Future News - 13 August 2024 14:53