Daily threat bulletin

13 September 2024

Vulnerabilities

GitLab warns of critical pipeline execution vulnerability

BleepingComputer - 12 September 2024 11:50

GitLab has released critical updates to address multiple vulnerabilities, the most severe of them (CVE-2024-6678) allowing an attacker to trigger pipelines as arbitrary users under certain conditions. [...]

Microsoft's September 2024 Patch Tuesday Addresses 4 Zero-Days, 79 Vulnerabilities

Security Boulevard - 12 September 2024 18:51

On September 10, 2024, Microsoft released its latest round of security updates as part of its monthly Patch Tuesday program. This month's updates address a total of 79 vulnerabilities across various Microsoft products, including four zero-day vulnerabilities that have been actively exploited in the wild.

Palo Alto Networks Patches Dozens of Vulnerabilities

SecurityWeek - 12 September 2024 14:09

Palo Alto Networks has fixed medium- and high-severity vulnerabilities in PAN-OS, Cortex XDR, ActiveMQ Content Pack, and Prisma Access Browser.

Cisco Patches High-Severity Vulnerabilities in Network Operating System

SecurityWeek - 12 September 2024 12:12

Cisco has announced security updates that patch eight vulnerabilities in IOS XR software, including six high-severity bugs.

Threat actors and malware

New Vo1d malware infects 1.3 million Android streaming boxes

BleepingComputer - 12 September 2024 18:10

Threat actors have infected over 1.3 million TV streaming boxes running Android with a new Vo1d backdoor malware, allowing the attackers to take full control of the devices. [...]

Fortinet confirms data breach after hacker claims to steal 440GB of files

BleepingComputer - 12 September 2024 15:01

Cybersecurity giant Fortinet has confirmed it suffered a data breach after a threat actor claimed to steal 440GB of files from the company's Microsoft Sharepoint server. [...]

Hackers targeting WhatsUp Gold with public exploit since August

BleepingComputer - 12 September 2024 13:27

Hackers have been leveraging publicly available exploit code for two critical vulnerabilities in the WhatsUp Gold network availability and performance monitoring solution from Progress Software. [...]

Iranian Cyber Group OilRig Targets Iraqi Government in Sophisticated Malware Attack

The Hacker News - 12 September 2024 17:19

Iraqi government networks have emerged as the target of an "elaborate" cyber attack campaign orchestrated by an Iran state-sponsored threat actor called OilRig.The attacks singled out Iraqi organizations such as the Prime Minister's Office and the Ministry of Foreign Affairs, cybersecurity company Check Point said in a new analysis.

'Hadooken' Malware Targets Oracle's WebLogic Servers

darkreading - 12 September 2024 21:58

An attacker is using the tool to deploy a cryptominer and the Tsunami DDoS bot on compromised systems.

Rising Tide of Software Supply Chain Attacks: An Urgent Problem

darkreading - 12 September 2024 15:00

Understanding a threat is just as important as the steps taken toward prevention.

UK related

UK NCA arrested a teenager linked to the attack on Transport for London

Security Affairs - 12 September 2024 20:49

U.K. police arrested a 17-year-old teenager allegedly linked to the cyberattack on London's public transportation agency, Transport for London. U.K.'s National Crime Agency announced the arrest of a 17-year-old teenager from Walsall who is allegedly linked to the cyberattack that recently hit Transport for London.

Irish Data Protection Regulator to Investigate Google AI

Infosecurity Magazine - 12 September 2024 17:15

Ireland's Data Protection Commission launches inquiry into whether Google followed GDPR rules over AI model training.

UK Recognizes Data Centers as Critical National Infrastructure

Infosecurity Magazine - 12 September 2024 12:30

The UK government has classified data centers as critical infrastructure in a move to protect UK data from cyber-attacks and prevent major IT blackouts.