Scottish Cyber Coordination Centre

Daily threat bulletin

9 July 2024

Vulnerabilities

Critical Ghostscript flaw exploited in the wild. Patch it now!

Security Affairs - 08 July 2024 19:12

Threat actors are exploiting Ghostscript vulnerability CVE-2024-29510 to bypass the sandbox and achieve remote code execution. Threat actors are actively exploiting a Ghostscript vulnerability, tracked as CVE-2024-29510, that can allow them to escape the SAFER sandbox and achieve remote code execution.

Critical Unpatched Flaws Disclosed in Popular Gogs Open-Source Git Service

The Hacker News - 08 July 2024 13:25

Four unpatched security flaws, including three critical ones, have been disclosed in the Gogs open-source, self-hosted Git service that could enable an authenticated attacker to breach susceptible instances, steal or wipe source code, and even plant backdoors.

Cisco Warns regreSSHion Vulnerability Impacts Multiple Products

Infosecurity Magazine - 08 July 2024 15:30

Cisco has told customers that 42 of its products are impacted by the OpenSSH regreSSHion vulnerability, with a further 51 products being investigated.

Threat actors and malware

Avast releases free decryptor for DoNex ransomware and past variants

BleepingComputer - 08 July 2024 15:51

Antivirus company Avast have discovered a weakness in the cryptographic schemeof the DoNex ransomware family and released a decryptor so victims can recover their files for free.

Mekotio Trojan Targets Latin American Banking Credentials

Infosecurity Magazine - 08 July 2024 16:30

A new analysis has shed light on the threat posed by the Mekotio banking trojan, a sophisticated piece of malware primarily targeting Latin American countries since at least 2015. Trend Micro said the trojan has been observed masquerading as communications from tax agencies.

CloudSorcerer - A new APT targeting Russian government entities

Securelist - 08 July 2024 08:00

Kaspersky discovered a new APT CloudSorcerer targeting Russian government entities and using cloud services as C2, just like the CloudWizard actor.

People's Republic of China (PRC) Ministry of State Security APT40 Tradecraft in Action

CISA Advisories -

This advisory outlines a People<92>s Republic of China (PRC) state-sponsored cyber group and their current threat. The advisory draws on the authoring agencies<92> shared understanding of the threat as well as ASD<92>s ACSC incident response investigations.

UK incidents

Hackers leak 39,000 print-at-home Ticketmaster tickets for 154 events

BleepingComputer - 08 July 2024 18:39

In an ongoing extortion campaign against Ticketmaster, threat actors have leaked almost 39,000 print-at-home tickets for 150 upcoming concerts and events, including Pearl Jam, Phish, Tate McCrae, and Foo Fighters. Ticketmaster responded by saying that the data is useless as their anti-fraud measures constantly rotate to unique mobile barcodes.