



Daily threat bulletin

5 July 2024

Vulnerabilities

[Apache fixed a source code disclosure flaw in Apache HTTP Server](#)

Security Affairs - 07 July 2024 18:20

The Apache Foundation addressed a critical source code disclosure vulnerability, tracked as CVE-2024-39884, in the HTTP Server. The Apache Software Foundation has addressed multiple vulnerabilities in its popular Apache HTTP Server. The vulnerabilities include denial-of-service (DoS), remote code execution, and unauthorized access issues.

[Latest Ghostscript vulnerability haunts experts as the next big breach enabler](#)

The Register - 05 July 2024 13:34

There's also chatter about whether medium severity scare is actually code red nightmare. Infosec circles are awash with chatter about a vulnerability in Ghostscript some experts believe could be the cause of several major breaches in the coming months.

Threat actors and malware

[New Eldorado ransomware targets Windows, VMware ESXi VMs](#)

BleepingComputer - 05 July 2024 12:56

A new ransomware-as-a-service (RaaS) called Eldorado emerged in March and comes with locker variants for VMware ESXi and Windows.

[Security Affairs Malware Newsletter: Round 1](#)

Security Affairs - 07 July 2024 15:07

Today marks the launch of the Security Affairs newsletter, specializing in Malware. Each week, it will feature a collection of the best articles and research on malware.

[New Golang-based Zergeca Botnet appeared in the threat landscape](#)

Security Affairs - 05 July 2024 10:39

Researchers uncovered a new Golang-based botnet called Zergeca that can carry out distributed denial-of-service (DDoS) attacks.

[GootLoader Malware Still Active, Deploys New Versions for Enhanced Attacks](#)

The Hacker News - 05 July 2024 15:10

The malware known as GootLoader continues to be in active use by threat actors looking to deliver additional payloads to compromised hosts. Updates to the GootLoader payload have



Scottish
Cyber
Coordination
Centre

resulted in several versions of GootLoader, with GootLoader 3 currently in active use," cybersecurity firm Cybereason said in an analysis published last week.

Hacker Stole Secrets From OpenAI

SecurityWeek - 05 July 2024 16:32

ChatGPT maker OpenAI was breached in 2023, but the company says source code and customer data were not accessed.

OVHcloud Sees Record 840 Mpps DDoS Attack

SecurityWeek - 05 July 2024 11:31

Cloud provider OVHcloud this week revealed that it had mitigated the largest ever distributed denial-of-service (DDoS) attack in terms of packet rate, amid an overall increase in DDoS attack intensity.

UK incidents

There's a new government in the UK. What can we expect from it on cyber?

The Record from Recorded Future News - 05 July 2024 21:09

Sir Keir Starmer, a former human rights lawyer who became one of the most senior public prosecutors in England and Wales before entering politics, was on Friday appointed the prime minister of the United Kingdom by Charles III and asked to form a government.