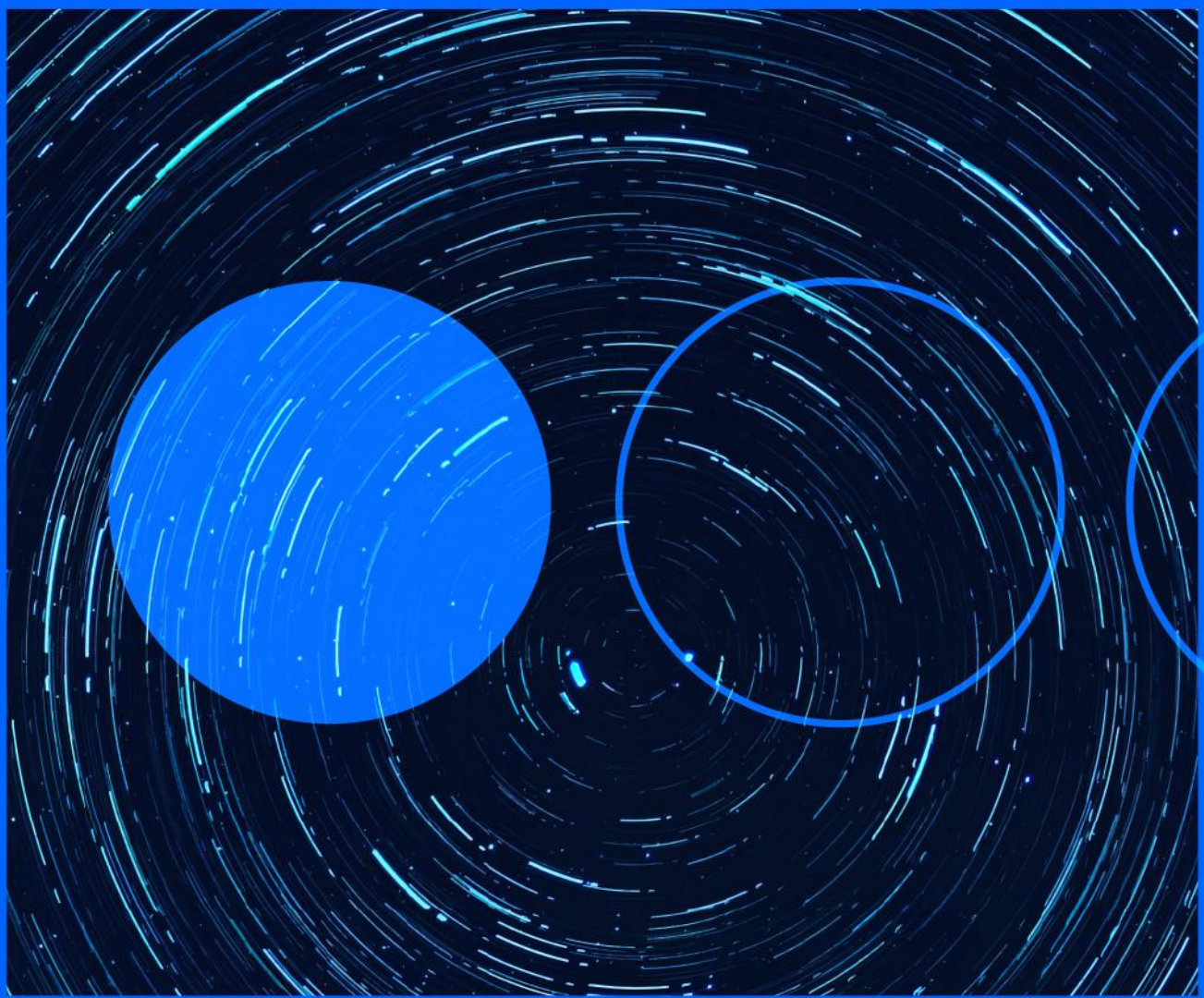
Telefónica Tech

14.04.2023

Cyber threats weekly briefing 2023



telefonicatech.com

Summary of the main attacks and vulnerabilities found by our experts in the last 7 days.

The icons stand for the following concepts:

				
Cyberoperations	Incidents	Malware	Information Leaks	Vulnerabilities

Apple fixes two new actively exploited 0-day vulnerabilities

INTERNATIONAL

Apple has released new security advisories about two new actively exploited 0-day vulnerabilities affecting iPhones, Macs and iPads. First, there is the security flaw registered as CVE-2023-28206, which is an out-of-bounds write to IOSurfaceAccelerator that could trigger data corruption, a crash or code execution. Secondly, the vulnerability assigned as CVE-2023-28205 is a use of WebKit that could allow data corruption or arbitrary code execution by reusing freed memory to create specially crafted malicious web pages controlled by threat actors. Apple recommends updating the software on affected devices to fix the two 0-day vulnerabilities in iOS 16.4.1, iPadOS 16.4.1, macOS Ventura 13.3.1 and Safari 16.4.1 versions.

URL: https://support.apple.com/en-us/HT213721

Microsoft Patch Tuesday includes an actively exploited 0-day vulnerability

INTERNATIONAL

In its latest security update, Microsoft has fixed a total of 98 vulnerabilities affecting several of its products, including Microsoft Windows, Office and Edge. These include an actively exploited 0-day vulnerability which has been registered as CVE-2023-28252, CVSSv3 of 7.8 according to the manufacturer. It is a CLFS flaw that could be exploited locally by malicious actors with the purpose of obtaining SYSTEM privileges. The rest of the critical security flaws, which have been registered as CVE-2023-28311, CVE-2023-21554 and CVE-2023-28231, CVE-2023-28219, CVE-2023-28220, CVE-2023-28250, CVE-2023-28291 should also be mentioned. The last vulnerabilities CVE-2023-28285, CVE-2023-28295, CVE-2023-28287 and CVE-2023-28311, although less critical than the rest, are worth mentioning and although they are not being actively exploited, they could be easily exploited by opening malicious documents sent in possible future phishing campaigns..

URL: https://msrc.microsoft.com/update-guide/releaseNote/2023-Apr

Quadreams accused of using spyware against political figures and journalists

INTERNATIONAL

Researchers from CitizenLab and Microsoft's Threat Intelligence team have published an investigation into the Israeli company QuaDreams, which they accuse of using spyware against journalists and political figures. The company's activity is allegedly based on the sale and distribution of a platform called Reign to government entities, described by Microsoft as a set of exploits, malware and infrastructure designed to exfiltrate information from mobile devices. Of the techniques used to operate it, researchers suspect it is a zero-click exploit for iOS devices, which they have named ENDOFDAYS, that would make use of invisible iCloud invitations. Analysis has identified at least five victims, who currently remain anonymous, in North America, Central Asia, Southeast Asia, Europe and the Middle East.

URL: https://citizenlab.ca/2023/04/spyware-vendor-quadream-exploits-victims-customers/

Android security bulletin for April

INTERNATIONAL

Android has released its security bulletin for the month of April, where it fixes a total of 68 vulnerabilities. Among the vulnerabilities, the most important ones are two detected in the System component, which have been catalogued as CVE-2023-21085 and CVE-2023-21096, both with critical severity, and which could allow a possible attacker to perform a remote code execution (RCE) without the need for additional execution privileges. In addition, four vulnerabilities in Qualcomm's closed source component have also been listed as critical: CVE-2022-33231, CVE-2022-33288, CVE-2022-33289 and CVE-2022-33302. Finally, a vulnerability in the Arm Mali GPU kernel driver, CVE-2022-38181 CVSSv3 8.8, has also been fixed which is reported to have been actively exploited.

URL: https://source.android.com/docs/security/bulletin/2023-04-01

Azure design flaw allows account takeover

INTERNATIONAL

An Orca investigation has exposed a design flaw in Microsoft Azure Shared Key that would allow an attacker to gain access to Microsoft Storage accounts. Although Orca has published a proof of concept demonstrating how to steal access tokens from higher privileged identities, move laterally, access critical business assets and execute remote code execution (RCE), Microsoft's Security Response Center has deemed the issue a design flaw and not a vulnerability, so it is unable to provide a security update and will have to wait for a redesign of Azure. In the meantime, it is recommended to remove shared key authorisation from Azure and instead adopt Azure Active Directory authentication as a mitigation strategy.

URL: https://orca.security/resources/blog/azure-shared-key-authorization-exploitation/

About Telefónica Tech

Telefónica Tech is the leading company in digital transformation. The company has a wide range of services and integrated technological solutions for Cybersecurity, Cloud, IoT, Big Data, or Blockchain.

More information

telefonicatech.com