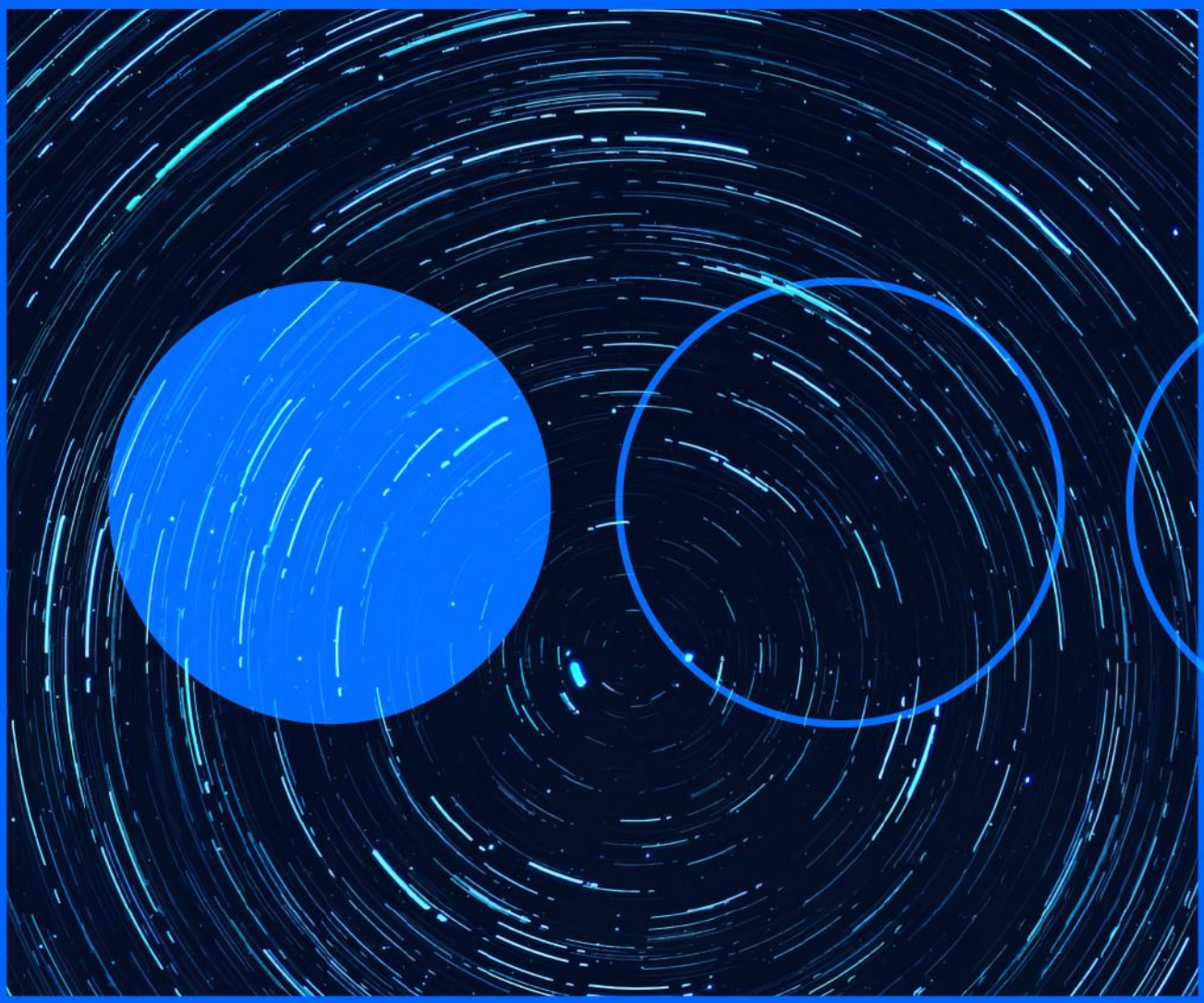
Telefónica Tech

17.02.2023

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 actively exploited 0-day

INTERNATIONAL

Apple has issued several security advisories to fix an actively exploited 0-day vulnerability. The security flaw, listed as CVE-2023-23529, is a type confusion in the browser's WebKit that could be used by a would-be attacker to execute arbitrary code on vulnerable devices after opening a malicious web page crafted for such purposes. This flaw affects both older and newer devices, being fixed in iOS 16.3.1 and iPadOS 16.3.1, macOS Ventura 13.2.1, and Safari 16.3.1. On the other hand, Apple has also fixed a vulnerability in the kernel that allows remote code execution, registered as CVE-2023-23514, which affected macOS Ventura devices and several iPhone and iPad models. Lastly, a vulnerability that could allow access to unprotected user data affecting macOS Ventura has been identified as CVE-2023-23522.

URL: https://support.apple.com/en-us/HT213635

Microsoft fixes 75 vulnerabilities in its Patch Tuesday including 3 0-days

INTERNATIONAL

Microsoft has patched 75 vulnerabilities in various products including Microsoft Windows, Office, Exchange and Azure in its latest security update. Nine of these vulnerabilities are reported to have received a critical severity score, and 66 others are reported to have been rated as "important". Three of these security bugs would be 0-day actively exploited: CVE-2023-21823, a remote code execution vulnerability in Windows Graphics Component with a CVSSv3 score of 7.8; CVE-2023-21715, a security feature bypass vulnerability in Microsoft Publisher with a CVSSv3 score of 7.3 and CVE-2023-23376, a privilege escalation vulnerability in Windows Common Log File System Driver with a CVSSv3 score of 7.8.

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

Cyber-attack against several NATO websites

INTERNATIONAL

A NATO official confirmed to the DPA news agency that the organisation was investigating a cyber-attack on several NATO websites. The attack took place on Sunday night and disabled several NATO websites, including that of the NATO Special Operations Headquarters. The attack was allegedly a politically motivated hacktivist action in favour of one of the parties in the current conflict, as a Telegram channel of a hacktivist group posted a message asking for help from fellow hackers to attack all NATO units. Other hacktivist channels also posted evidence of inoperable NATO assets such as the Military Command website and the Joint Military Centre website, among others.

URL: https://www.europapress.es/internacional/noticia-varias-webs-otan-sufren-ataque-informatico-20230213010251.html

Mozilla issues security updates for Firefox 110 and Firefox ESR

INTERNATIONAL

Mozilla has issued two security alerts regarding vulnerability fixes in Firefox110 and FirefoxESR. Most of these vulnerabilities, still pending CVSS classification, have been categorised by the vendor as high impact. Their exploitation could lead an attacker to perform spoofing attacks; access confidential information, including NTLM credentials; evade security mechanisms or execute arbitrary code, among other behaviours. The vendor recommends upgrading to the latest version of Firefox 110 and Firefox ESR 102.8. The US Cybersecurity and Infrastructure Security Agency (CISA) has issued a notification informing of these updates and requesting users and administrators to implement the necessary measures.

URL: https://www.mozilla.org/en-US/security/advisories/mfsa2023-05/

Vulnerabilities in Schneider Electric PLC models

INTERNATIONAL

- Forescout's team of Vedere Labs researchers has published an analysis of two critical vulnerabilities affecting several Schneider Electric PLC models. These security flaws are the one registered as CVE-2022-45789, with a CVSSv3 9.8, which allows an authentication bypass that could cause the execution of unauthorised Modbus functions on the controller by hijacking an authenticated Modbus session. In addition, the vulnerability registered as CVE-2022-45788, which has also been assigned a CVSSv3 of 9.8, could be exploited for remote code execution, cause a denial of service attack and could result in loss of confidentiality and data integrity when executing undocumented Modbus

UMAS CSA commands. Researchers indicate that malicious actors could chain exploit them to achieve lateral movement in the victim's network. The affected versions include all versions of EcoStruxure Control Expert and Modicon Unity PLC, as well as EcoStruxure Process Expert version V2020.

URL: https://www.forescout.com/blog/deep-lateral-movement-in-ot-networks-when-is-a-perimeter-not-a-perimeter/

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