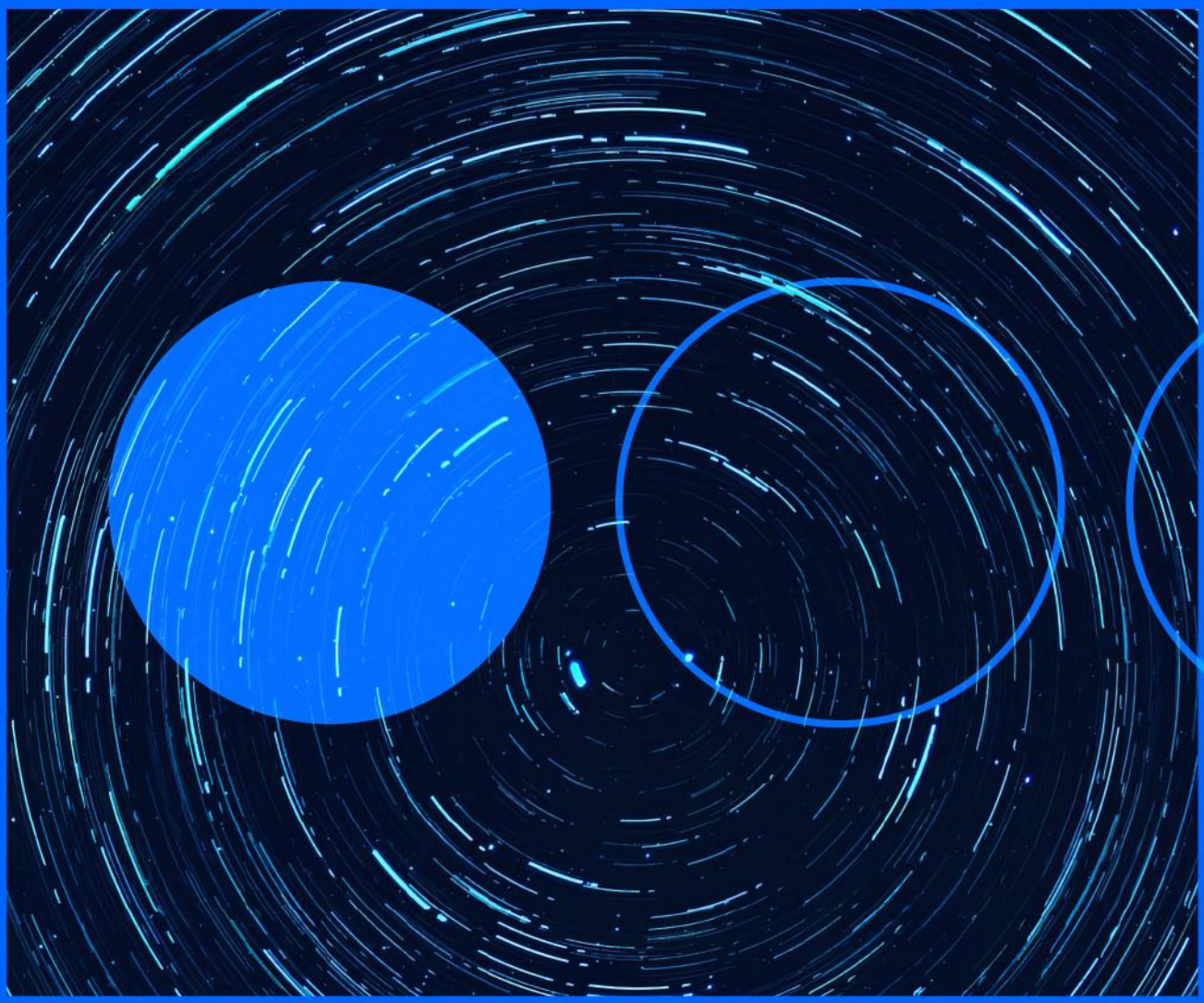
Telefónica Tech

09.09.2022

Cyber threats weekly briefing 2022



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

0-day vulnerability in Google Chrome

INTERNATIONAL

Google released on Friday an emergency patch for the Chrome browser on Windows, Mac and Linux, fixing a 0-day vulnerability, which is being actively exploited. The security flaw, identified as CVE-2022-3075, relates to insufficient data validation by the Mojo library collection, which is responsible for providing independent mechanisms for communication between processes with different programming languages. A malicious actor could bypass the security restrictions when the victim accessed a specially crafted web page. Google reported that an anonymous researcher reported the vulnerability on August 30 and that exploits are available to exploit it. Users of Chromium-based browsers, such as Microsoft Edge, Brave and Opera, would be affected by this vulnerability, so it is recommended to upgrade to Google Chrome version 105.0.5195.102, which addresses the 0-day.

https://chromereleases.googleblog.com/2022/09/stable-channel-update-for-desktop.html

New breach affects the giant Samsung

INTERNATIONAL

The multinational company Samsung acknowledged on September the 2nd that it had been the target of a security breach. According to the statement issued, at the end of July, an unauthorised third party gained access to information on some Samsung systems in the United States, exposing the personal information of several customers. The information accessed included name, demographic and contact information, date of birth, and product registration information, but did not include social security numbers or credit card information. This incident is the second in less than six months to be reported, as in March there were reports that internal data from the source code of its smartphones was leaked [1]. The company has indicated that it has taken security measures to ensure that such incidents do not happen again.

[1] https://www.bloomberg.com/news/articles/2022-03-07/samsung-says-hackers-breached-company-data-galaxy-source-code

QNAP patches 0-day used in new Deadbolt ransomware attacks

INTERNATIONAL

QNAP has issued a security advisory urging NAS users to upgrade to the latest version of Photo Station. The advisory follows the detection of an ongoing DeadBolt ransomware attacks that began on Saturday that exploits a 0-day vulnerability in Photo Station. QNAP, which has already released security updates for Photo Station, urges its customers to update the software to the latest available version and suggests that users replace Photo Station with QuMagie, a safer photo storage management tool for QNAP NAS devices. The details of this flaw are still unclear at this time, but the company strongly recommends, in order to reduce the possibility of being attacked, not to connect QNAP NAS directly to the Internet and to make use of the myQNAPcloud Link feature provided by QNAP, or enable the VPN service. They also recommend using strong passwords for user accounts and take regular backups to prevent data loss. This would be the fourth round of DeadBolt attacks targeting QNAP devices since January 2022, which was followed by similar incursions in May and June.

https://www.qnap.com/en/security-advisory/qsa-22-24

HP fixes a serious vulnerability in HP Support Assistant

INTERNATIONAL

HP has issued a security advisory warning users about a recently discovered vulnerability in HP Support Assistant, a software tool that comes pre-installed on all HP computers, which is used for troubleshooting or performing hardware diagnostic tests, among others. The flaw, identified as CVE-2022-38395 and with CVSS of 8.2, allows attackers to elevate their privileges on vulnerable systems. Although the manufacturer has not provided many details about the vulnerability, the advisory mentions that it is a DLL hijacking flaw when users try to launch HP Performance Tune-up from HP Support Assistant. In this type of flaw, the code that is executed when loading the library obtains the privileges of the executable, in this case SYSTEM permissions. Due to the large number of devices with HP Support Assistant installed and the low complexity of the exploit, it is recommended that all HP users update Support Assistant as soon as possible.

https://support.hp.com/us-en/document/ish_6788123-6788147-16/hpsbhf03809

HP corrige una vulnerabilidad grave en HP Support Assistant

INTERNACIONAL

VF Corporation has released a statement to its customers in which they report that they have suffered a data breach on The North Face and Vans retail brands. The threat actors used credential stuffing techniques to

breach 162,823 customer accounts on thenorthface.com and 32,082 customer accounts on vans.com. A credential stuffing attack involves attempting to access accounts with compromised credentials from other leaks, a strategy that is based on the assumption that the users are probably reusing passwords across multiple platforms. The attack on The North Face began on July 26th, was detected on August 11th and disrupted on August 19th. On the other hand, the intrusion at Vans was detected on the 20th of August and was active for only one day. Among the data that could have been exfiltrated were names, addresses, e-mail addresses, purchase history and customer telephone numbers, among others. In their statement, the company said that credit card data is stored in third-party payment systems, so it could not have been affected by the attack. Finally, the company has confirmed that all the credentials of the affected accounts have been reset.

https://www.documentcloud.org/documents/22275912-consumer-notification-template-vans_northface_combined-2022

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