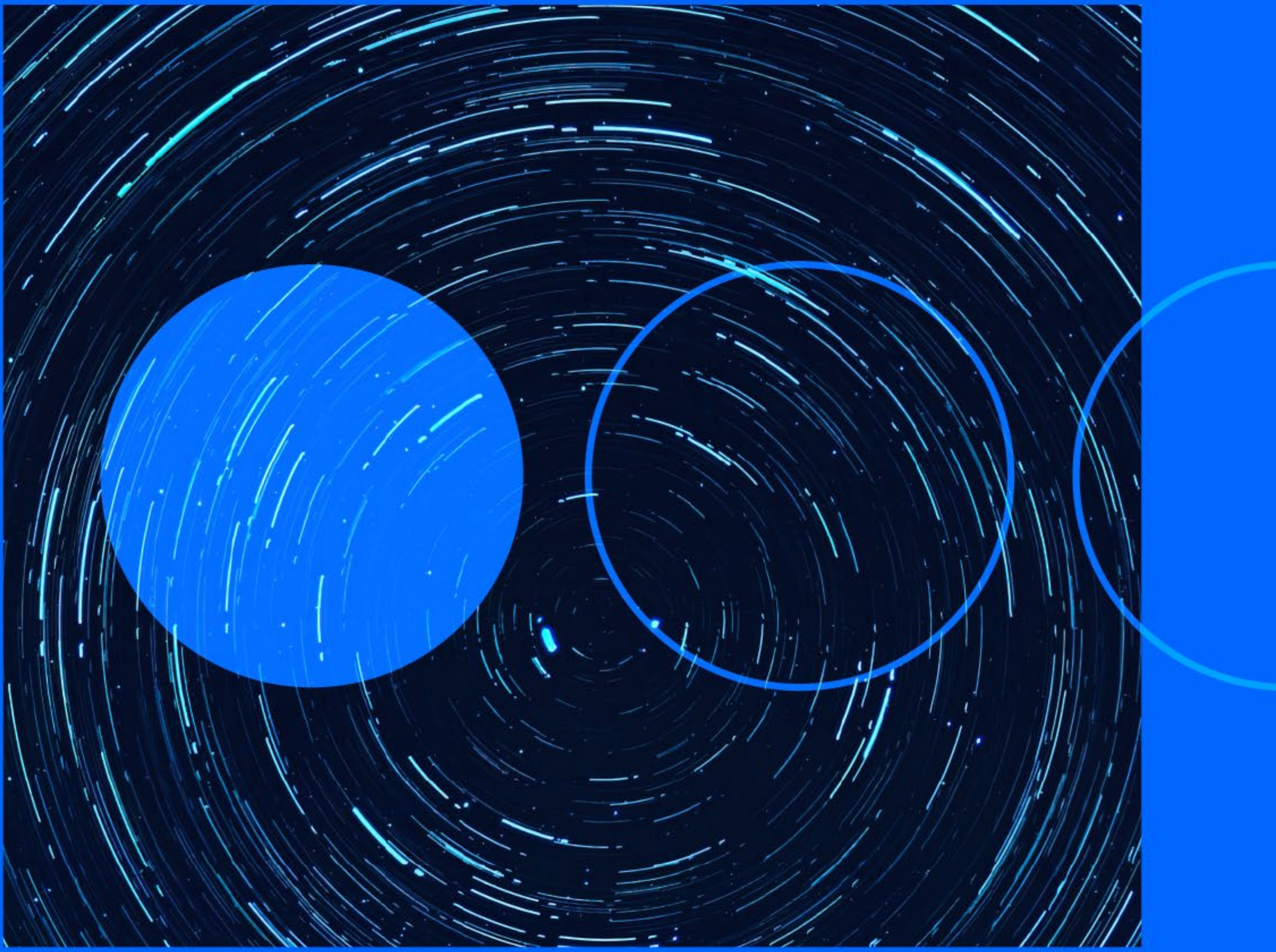
Telefónica
Tech

09.12.2022

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

Ninth Chrome 0-day of the year

INTERNATIONAL

Google has released Chrome 108.0.5359.94 for Mac and Linux, and 108.0.5359.94/.95 for Windows, which fixes a 0-day vulnerability, the ninth detected in Chrome this year. Catalogued as CVE-2022-4262 with a high criticality according to Google, it is described as Type confusion in V8 in Google Chrome, for versions prior to 108.0.5359.94. Exploitation of this security flaw could allow a remote attacker to potentially exploit stack corruption via a manipulated HTML page. Google has not provided further details of this flaw detected by Clement Lecigne of Google's Threat Analysis Group on 29 November, until most users have updated their browsers. It is worth noting that the security advisory published by the company reports that an exploit for this vulnerability currently exists.

URL: https://chromereleases.googleblog.com/2022/12/stable-channel-update-for-desktop.html

RCE vulnerability in Visual Studio Code

INTERNATIONAL

Google security researcher Thomas Shadwell has identified an important vulnerability in Visual Studio Code. This security flaw, identified as CVE-2022-41034, with a CVSSv3 of 7.8, could allow malicious actors to perform remote code execution, making it possible to take control of the victim's computer. The methodology used to carry out the attack consists of forwarding a link to a website in order to take over a Visual Studio Code user's computer and any other device connected through Visual Studio Code's remote development feature. According to the researcher, this issue affects GitHub Codespaces, github.dev and Visual Studio Code web and desktop versions. It should be noted that this remote code execution vulnerability affects VS Code 1.71 and earlier versions. It is also recommended to apply the patch released by Microsoft to fix this security flaw.

URL: https://github.com/google/security-research/security/advisories/GHSA-pw56-c55x-cm9m

Vulnerability in NETGEAR routers patched urgently

INTERNATIONAL

Within the context of Pwn20wn Toronto 2022, a bug hunting competition that has been held as part of the CanSecWest security conference since 2007, the manufacturer of NETGEAR devices has been forced to patch a vulnerability as a matter of urgency. In this regard, researchers at Tenable have published an article in which, based on code published by NETGEAR to mitigate the vulnerability in NETGEAR Nighthawk WiFi6 Router (RAX30 AX2400 series) devices, they reveal details of the patched bug, namely a configuration error at the network level whereby access restriction policies were not being applied correctly to the devices when they had an exposed IPv6 interface. The vulnerability, which at the time of writing has not yet been assigned a CVE, would be mitigated with the update proposed by the manufacturer to versions 1.0.9.90 and later. Following Tenable's indications, it is recommended to perform the manual check since devices with versions higher than v1.0.6.74 would not be able to auto-update automatically.

URL: https://medium.com/tenable-techblog/netgear-router-network-misconfiguration-70ac695c81a6

High severity vulnerability in Cisco IP phone devices

INTERNATIONAL

Cisco has issued a security advisory warning of a high-severity vulnerability affecting several models of its branded IP phone devices. The security flaw, catalogued as CVE-2022-20968, and with a CVSSv3 of 8.1 could allow a malicious actor to cause a stack overflow, triggering a remote code execution or denial of service (DoS) attack. While the company's security incident response team is aware of the existence of a proof of concept, they have no evidence that it has been exploited in attacks. It should be noted that Cisco has indicated that it will release a security patch next January 2023, and that until then it recommends a series of mitigation tips by disabling Cisco's discovery protocol on the affected devices, which are IP Phone 7800 and 8800 Series running firmware version 14.2 and earlier.

URL: https://www.forescout.com/blog/oticefall-continues-vedere-labs-discloses-three-new-vulnerabilities-affecting-ot-products-how-to-mitigate/

Zombinder: app repackaging service containing malware

INTERNATIONAL

Researchers at ThreatFrabric have published an article detailing the existence of a service on the dark web, which they have named Zombinder, that allows threat actors to add malware to legitimate apps in order to evade security controls. The researchers point out that applications repackaged with Zombinder are 100 per cent compliant with their original purpose, so the victim does not suspect that they have been infected with malicious software, usually of the stealer type. ThreatFrabric reports that they have mainly identified the clipper called "Laplas" and well-known information stealers such as "Ermac", "Erbium" and "Aurora" in applications modified by Zombinder. Finally, the service targets Windows and Android operating system app users.

URL: https://www.threatfabric.com/blogs/zombinder-ermac-and-desktop-stealers.html

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

The information disclosed in this document is the property of Telefónica Cybersecurity & Cloud Tech S.L.U. ("Telefónica Tech") and/or any other entity within Telefónica Group and/or its licensors. Telefónica Tech and/or any Telefonica Group entity or Telefónica Tech's licensors reserve all patent, copyright and other proprietary rights to this document, including all design, manufacturing, reproduction, use and sales rights thereto, except to the extent said rights are expressly granted to others. The information in this document is subject to change at any time, without notice.
Neither the whole nor any part of the information contained herein may be copied, distributed, adapted or reproduced in any material form except with the prior written consent of Telefónica Tech.
This document is intended only to assist the reader in the use of the product or service described in the document. In consideration of receipt of this document, the recipient agrees to use such information for its own use and not for other use.
Telefónica Tech shall not be liable for any loss or damage arising out from the use of the any information in this document or any error or omission in such information or any incorrect use of the product or service. The use of the product or service described in this document are regulated in accordance with the terms and conditions accepted by the reader.
Telefónica Tech and its trademarks (or any other trademarks owned by Telefónica Group) are registered service marks.