Cloud Consultancy

DIGITALIZATION & SECURITY

CCDS CYBER SECURITY PICKS

44th Release November 2022

Google Rolls Out New Chrome Browser Update to Patch Yet Another Zero-Day Vulnerability

Search giant Google on Friday released an out-of-band security update to fix a new actively exploited zero-day flaw in its Chrome web browser.
The high-severity flaw, tracked as CVE-2022-4262, concerns a type confusion bug in the V8 JavaScript engine. Clement Lecigne of Google's Threat Analysis Group (TAG) has been credited with reporting the issue on November 29, 2022.

Type confusion vulnerabilities could be weaponized by threat actors to perform out-of-bounds memory access, or lead to a crash and arbitrary code execution.

Source:https://thehackernews.com/2022/12/google-rolls-out-new-chrome-browser.html

Hive Ransomware Attackers Extorted $100 Million from Over 1,300 Companies Worldwide

The threat actors behind the Hive ransomware-as-a-service (RaaS) scheme have launched attacks against over 1,300 companies across the world, netting the gang $100 million in illicit payments as of November 2022.
"Hive ransomware has targeted a wide range of businesses and critical infrastructure sectors, including government facilities, communications, critical manufacturing, information technology, and — especially — Healthcare and Public Health (HPH)," U.S. cybersecurity and intelligence authorities said in an alert.

Source:https://thehackernews.com/2022/11/hive-ransomware-attackers-extorted-100.html

Citrix Issues Patches for Critical Flaw Affecting ADC and Gateway Products

Citrix has released security updates to address a critical authentication bypass flaw in the application delivery controller (ADC) and Gateway products that could be exploited to take control of affected systems.

Successful exploitation of the issues could enable an adversary to gain authorized access, perform remote desktop takeover, and even circumvent defenses against login brute-force attempts under specific configurations.

Source:https://thehackernews.com/2022/11/citrix-issues-patches-for-critical-flaw.html

BY MUHAMMED RAFEEK (CYBER SECURITY ANALYST – SOC TEAM)

Google Accuses Spanish Spyware Vendor of Exploiting Chrome, Firefox, & Windows Zero-Days

A Barcelona-based surveillanceware vendor named Variston IT is said to have surreptitiously planted spyware on targeted devices by exploiting several zero-day flaws in Google Chrome, Mozilla Firefox, and Windows, some of which date back to December 2018.
"Their Heliconia framework exploits n-day vulnerabilities in Chrome, Firefox, and Microsoft Defender, and provides all the tools necessary to deploy a payload to a target device," Google Threat Analysis Group (TAG) researchers Clement Lecigne and Benoit Sevens said in a write-up.Source:https://thehackernews.com/2022/09/microsoft-confirms-2-new-exchange-zero.html

Hackers Using Trending TikTok 'Invisible Challenge' to Spread Malware

Threat actors are capitalizing on a popular TikTok challenge to trick users into downloading information-stealing malware, according to new research from Checkmarx.

The trend, called Invisible Challenge, involves applying a filter known as Invisible Body that just leaves behind a silhouette of the person's body.The TikTok videos posted by the attackers, @learncyber and @kodibtc, on November 11, 2022, are estimated to have reached over a million views. The accounts have been suspended.

Source:https://thehackernews.com/2022/11/hackers-using-trending-invisible.html

All You Need to Know About Emotet in 2022

Emotet is by far one of the most dangerous trojans ever created. The malware became a very destructive program as it grew in scale and sophistication. The victim can be anyone from corporate to private users exposed to spam email campaigns.

The botnet distributes through phishing containing malicious Excel or Word documents. When users open these documents and enable macros, the Emotet DLL downloads and then loads into memory.

It searches for email addresses and steals them for spam campaigns. Moreover, the botnet drops additional payloads, such as Cobalt Strike or other attacks that lead to ransomware.

To overcome malware's anti-evasion techniques and capture the botnet – use a malware sandbox as the most convenient tool for this goal. In ANY.RUN, you can not only detect, monitor, and analyze malicious objects but also get already extracted configurations from the sample.

Source: https://thehackernews.com/2022/11/all-you-need-to-know-about-emotet-in.html

Watch Out! These Android Keyboard Apps With 2 Million Installs Can be Hacked Remotely

Multiple unpatched vulnerabilities have been discovered in three Android apps that allow a smartphone to be used as a remote keyboard and mouse.

The apps in question are Lazy Mouse, PC Keyboard, and Telepad, which have been cumulatively downloaded over two million times from the Google Play Store. Telepad is no longer available through the app marketplace but can be downloaded from its website.

"These three applications are widely used but they are neither maintained nor supported, and evidently, security was not a factor when these applications were developed," Synopsys security researcher Mohammed Alshehri said.

Source:https://thehackernews.com/2022/12/watch-out-these-android-keyboard-apps.html

Cloud Consultancy

Cloud Consultancy for Digitalization & Security – CCDS's is a Specialized Company in IT and Information Security Services, which has its international headquarters in the UAE. It also has branch offices throughout the MENA Region with its premier office in Saudi Arabia. Innovative and professional in its approach, it always partners with best-in-class products and services, to identify and solve security threats and issues for its clients.

Contact Us