Cloud Consultancy
DIGITALIZATION & SECURITY

CCDS CYBER SECURITY PICKS

45th Release December 2022

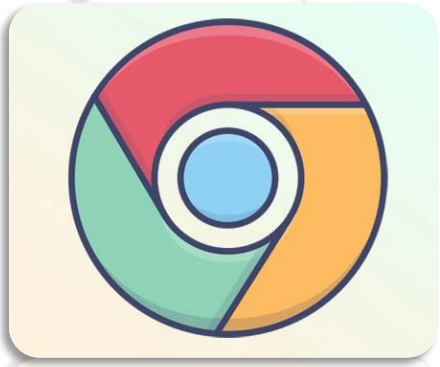
Fortinet Warns of Active Exploitation of New SSL-VPN Pre-auth RCE Vulnerability

Fortinet issued emergency patches for a severe security flaw affecting its FortiOS SSL-VPN product that it said is being actively exploited in the wild.

Tracked as CVE-2022-42475 (CVSS score: 9.3), the critical bug relates to a heap-based buffer overflow vulnerability that could allow an unauthenticated attacker to execute arbitrary code via specially crafted requests.

The company said it's "aware of an instance where this vulnerability was exploited in the wild," urging customers to move quickly to apply the updates.

Source:https://thehackernews.com/2022/12/fortinet-warns-of-active-exploitation.html



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

Search giant Google 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

Cybercrime (and Security) Predictions for 2023

Here's a look at how cybercrime will evolve in 2023 and what you can do to secure and protect your organization in the year ahead.

Increase in digital supply chain attacks

Mobile-specific cyber threats are on-the-rise

Double down on cloud security Ransomware-as-a-Service is here to stay

Data privacy laws are getting stricter—get ready

Source:https://thehackernews.com/2022/12/cybercrime-and-security-predictions-for.html#increase-in-digital-supply-chain-attacks

New Malvertising Campaign via Google Ads Targets Users Searching for Popular Software

Users searching for popular software are being targeted by a new malvertising campaign that abuses Google Ads to serve trojanized variants that deploy malware, such as Raccoon Stealer and Vidar.

The activity makes use of seemingly credible websites with typosquatted domain names that are surfaced on top of Google search results in the form of malicious ads by hijacking searches for specific keywords.

Source:https://thehackernews.com/2022/12/new-malvertising-campaign-via-google.html

APT Hackers Turn to Malicious Excel Add-ins as Initial Intrusion Vector

Microsoft's decision to block Visual Basic for Applications (VBA) macros by default for Office files downloaded from the internet has led many threat actors to improvise their attack chains in recent months.

Now according to Cisco Talos, advanced persistent threat (APT) actors and commodity malware families alike are increasingly using Excel add-in (.XLL) files as an initial intrusion vector.

Source:https://thehackernews.com/2022/12/apt-hackers-turn-to-malicious-excel-add.html

Top 5 Web App Vulnerabilities and How to Find Them

According to recent research from Verizon, web application attacks are involved in 26% of all breaches, and app security is a concern for ¾ of enterprises.

What are the common vulnerabilities?

1 — SQL injection

2 — XSS (cross-site scripting)

3 — Path traversal

4 — Broken authentication

5 — Security misconfiguration

How to test for vulnerabilities?

Web security testing for applications is usually split into two types – vulnerability scanning and penetration testing

Source: https://thehackernews.com/2022/12/top-5-web-app-vulnerabilities-and-how.html

France Fines Microsoft €60 Million for Using Advertising Cookies Without User Consent

France's privacy watchdog has imposed a €60 million ($63.88 million) fine against Microsoft's Ireland subsidiary for dropping advertising cookies in users' computers without their explicit consent in violation of data protection laws in the European Union.

The Commission nationale de l'informatique et des libertés (CNIL) noted that users visiting the home page of its Bing search engine did not have a "mechanism to refuse cookies as easily as accepting them."

Along with the fines, Microsoft has also been ordered to alter its cookie practices within three months, or risk facing an additional penalty of €60,000 per day of non-compliance following the end of the time period.

Source:https://thehackernews.com/2022/12/france-fines-microsoft-60-million-for.html

Contact Us

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.