Cloud Consultancy
DIGITALIZATION & SECURITY

CCDS CYBER SECURITY PICKS

43rd Release October 2022

Microsoft Confirms Server Misconfiguration Led to 65,000+ Companies' Data Leak

Microsoft confirmed that it inadvertently exposed information related to thousands of customers following a security lapse that left an endpoint publicly accessible over the internet sans any authentication. This misconfiguration resulted in the potential for unauthenticated access to some business transaction data corresponding to interactions between Microsoft and prospective customers, such as the planning or potential implementation and provisioning of Microsoft services. The misconfiguration of the Azure Blob Storage was spotted on September 24, 2022, by cybersecurity company SOCRadar.
Source:https://thehackernews.com/2022/10/microsoft-confirms-server.html

Google Issues Urgent Chrome Update to Patch Actively Exploited Zero-Day Vulnerability

Google on Thursday rolled out emergency fixes to contain an actively exploited zero-day flaw in its Chrome web browser.

The vulnerability, tracked as CVE-2022-3723, has been described as a type confusion flaw in the V8 JavaScript engine. CVE-2022-3723 is the third actively exploited type confusion bug in V8 this year after CVE-2022-1096 and CVE-2022-1364. Users are recommended to upgrade to version 107.0.5304.87 for macOS and Linux and 107.0.5304.87/.88 for Windows to mitigate potential threats.
Source:https://thehackernews.com/2022/10/google-issues-urgent-chrome-update-to.html

Researchers Say Microsoft Office 365 Uses Broken Email Encryption to Secure Messages

New research has disclosed what's being called a security vulnerability in Microsoft 365 that could be exploited to infer message contents due to the use of a broken cryptographic algorithm.

The [Office 365 Message Encryption] messages are encrypted in insecure Electronic Codebook (ECB) mode of operation Office 365 Message Encryption (OME) is a security mechanism used to send and receive encrypted email messages between users inside and outside an organization without revealing anything about the communications themselves.
Source:https://thehackernews.com/2022/10/researchers-claim-microsoft-office-365.html

Over 280,000 WordPress Sites Attacked Using WPGateway Plugin Zero-Day Vulnerability

A zero-day flaw in the latest version of a WordPress premium plugin known as WPGateway is being actively exploited in the wild, potentially allowing malicious actors to completely take over affected sites.Part of the plugin functionality exposes a vulnerability that allows unauthenticated attackers to insert a malicious administrator.

The most common indicator that a website running the plugin has been compromised is the presence of an administrator with the username "rangex."

Source:https://thehackernews.com/2022/09/microsoft-confirms-2-new-exchange-zero.html

Fortinet Warns of Active Exploitation of Newly Discovered Critical Auth Bypass Bug

Fortinet revealed that the newly patched critical security vulnerability impacting its firewall and proxy products is being actively exploited in the wild.the flaw relates to an authentication bypass in FortiOS, FortiProxy, and FortiSwitchManager that could allow a remote attacker to perform unauthorized operations on the administrative interface via specially crafted HTTP(S) requests. Updates have been released by the security company in FortiOS versions 7.0.7 and 7.2.2, FortiProxy versions 7.0.7 and 7.2.1, and FortiSwitchManager version 7.2.1.

Source:https://thehackernews.com/2022/10/fortinet-warns-of-active-exploitation.html

Former Uber Security Chief Found Guilty of Data Breach Coverup

A U.S. federal court jury has found former Uber Chief Security Officer Joseph Sullivan guilty of not disclosing a 2016 breach of customer and driver records to regulators and attempting to cover up the incident.

Sullivan has been convicted on two counts: One for obstructing justice by not reporting the incident and another for misprision. He faces a maximum of five years in prison for the obstruction charge, and a maximum of three years for the latter.

“We expect those companies to protect that data and to alert customers and appropriate authorities when such data is stolen by hackers. Sullivan affirmatively worked to hide the data breach from the Federal Trade Commission and took steps to prevent the hackers from being caught”

U.S. Attorney Stephanie M. Hinds said in a press statement.

Source: https://thehackernews.com/2022/10/former-uber-security-chief-found-guilty.html

How to keep your data safe while surfing the web

#1 Stay away from weak passwords. Make sure they are strong and complex by incorporating both upper and lowercase letters, numbers and punctuation marks. Keep a unique password for each account and never use the same password for multiple accounts.

#2 Web browsers are a perfect source for fraud, spyware and phishing attempts, but also for advertisers to track your activity. Make sure they are updated and that you are using the latest version. Never click on suspicious pop-ups and double check that all websites you access are https, which means they are secured through SSL/TLS encryption.

#3 Shopping online? Great! But watch credit card theft and financial fraud are increasing, so be mindful when making online payments. Once again, make sure the payment is run through an encrypted https website.

Source:https://www.bitdefender.com/blog/hotforsecurity/how-to-keep-your-data-safe-while-surfing-the-web

Cloud Consultancy

Contact Us

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.