December 5, 2022

INFOSEC WEEKLY

#MADE4SECURITY

- Google rolls out new chrome browser update to patch yet another zero-day vulnerability
- Researchers find a way malicious NPM libraries can evade vulnerability detection
- Android Keyboard Apps with 2 million+ downloads can get hacked remotely
- Researchers Detail AppSync Cross-Tenant Vulnerability in Amazon Web Services
- Cisco ISE vulnerabilities can be chained in One-Click exploit

CryptoGen Nepal

Introduction to InfoSec Weekly

InfoSec Weekly is a compilation of security related news feed that aims to update the readers about cyber security, cyber threats, malware attacks, new technologies and cyber security awareness every week. We primarily cover events and news related to offensive side of the Information Security such as hacking, password and sensitive information leakage, new vulnerabilities and important CVE's that can impact an individual or an organization. We also aim to provide defensive tactics to overcome known vulnerabilities that can protect organizations and individuals from any attacks.

Our main aim is to spread awareness regarding various cyber related threats.

About Us

We are a team of security enthusiasts with an aim to provide various Information Security Services to organizations. Our company aims to provide professional grade cyber security solutions for all your Information Technology infrastructures. Our team has been demonstrating penetration testing skills using methodologies such as OSSTMM, NIST and OWASP. We aim to help companies protect their valuable data from any internal or external threats. Our team members have been practicing their skills to detect and report vulnerabilities in a live environment. Organizations such as Google, Facebook, Twitter, Yahoo!, eBay, eset, BugCrowd, under armour, Coinbase, CCM, etc. have recognized our team members for reporting vulnerabilities and have helped these organizations from malicious users. Our team's professional work experience consists of various Government organizations, National and International based private organizations, INGOs, etc. Our Services ranges from VAPT, Incident Response, Information Security Training, Endpoint threat analysis, Cyber security consultant, etc.

Google rolls out new chrome browser update to patch yet another zero-day vulnerability

Description	
Google, a leading search engine, fixed a newly discovered and actively exploited zero-day vulnerability in its Chrome web browser on Friday. The high-severity issue affects a type of confusion bug in the V8 JavaScript engine and is tagged as CVE-2022-4262. Threat actor can exploit the flaw to execute arbitrary code, crash or get access to out-of-bound memory. The National Vulnerability Database of NIST states that the vulnerability potentially allows a remote attacker to possibly exploit heap corruption through a manipulated HTML page.	
Source	https://thehackernews.com/2022/12/google-rolls-out-new-chrome-browser.html
Infected Technology	Chrome Web Browser
Recommendation	Update to versions 108.0.5359.94 for macOS and Linux and 108.0.5359.94/.95 for Windows.
CVE_ID	CVE-2022-4262

Researchers find a way malicious NPM libraries can evade vulnerability detection

Description	
On Monday, the U.S. Cyber Security, and Infrastructure Security Agency (CISA), citing evidence of ongoing exploitation, added a significant vulnerability affecting Oracle Fusion Middleware to its Known Exploited Vulnerabilities (KEV) catalog. The threat actor who successfully exploits the vulnerability using remote command execution can compromise the network and take control of Access Manager instances. By December 19, 2022, federal agencies must apply the vendor patches to protect their networks from potential threats.	
Source	https://thehackernews.com/2022/11/researchers-find-way-malicious-npm.html
Infected Technology	Oracle Fusion Middleware
Recommendation	Apply the security patch immediately after the vendor releases for their product.
CVE_ID	CVE-2021-35587

Android Keyboard Apps with 2 million+ downloads can get hacked remotely

Description	
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. While the Synopsys Cybersecurity Research Center (CyRC) discovered up to seven flaws related to weak or missing authentication, missing authorization, and insecure communication in these apps, which connect to a server on a desktop and transmit mouse and keyboard events to it, these apps do so with several security flaws. In a nutshell, the vulnerabilities (CVE-2022-45477 through CVE-2022-45483) might be used by an attacker to run arbitrary commands without authentication or collect sensitive data by exposing users' keystrokes in cleartext. The Lazy Mouse server also has a weak password policy and doesn't use rate limiting, which makes it easy for remote, unauthenticated attackers to brute force the PIN and issue malicious commands.	
Source	https://thehackernews.com/2022/12/watch-out-these-android-keyboard-apps.html
Infected Technology	Android Application
Recommendation	Uninstall or trying an alternative solution
CVE_ID	CVE-2022-45483 CVE-2022-45477

Researchers Detail AppSync Cross-Tenant Vulnerability in Amazon Web Services

Description	
A cross-tenant vulnerability in the platform of Amazon Web Services has been patched, preventing an attacker from using it to access resources without authorization. There is a kind of privilege escalation when there is an issue with an uncertain deputy. Datadog informed AWS of the vulnerability on September 1, 2022, and on September 6 a remedy was made available. Due to a vulnerability in AWS AppSync, according to Frichette, "attackers were able to overcome account boundaries and perform AWS API requests in victim accounts" by using IAM roles that trusted the AppSync service. By using this method to hack AppSync-using companies, attackers may be able to access the resources required by such jobs. According to Amazon, the flaw had no impact on the customers).	
Source	https://thehackernews.com/2022/11/researchers-detail-appsync-cross-tenant.html
Infected Technology	Amazon Web Services
Recommendation	Keeping software up to date

Schoolyard Bully Trojan Apps Stole Facebook Credentials from Over 300,000 Android Users

Description	
The Schoolyard Bully Trojan, a new Android threat campaign, has infected more than 300,000 users in 71 countries. The spyware, which is primarily meant to steal Facebook passwords, poses as legitimate education-themed apps in order to trick unwary users into downloading it. The apps have since been removed from the official Google Play Store, where they were previously accessible for download. Despite this, they are still accessible through independent app stores. This trojan uses JavaScript injection to steal the Facebook credentials. To do this, it launches the Facebook login page in a WebView and embeds malicious JavaScript code inside to exfiltrate the user's contact information—including phone number, email address, and password—to a set-up command-and-control (C2) server. To prevent detection by antivirus software, the Schoolyard Bully Trojan also takes use of native libraries such as "libabc.so" while the virus targets Vietnamese language apps, it has also been identified in several other apps accessible in over 70 countries, highlighting the scope of the assaults.	
Source	https://thehackernews.com/2022/12/schoolyard-bully-trojan-apps-stole.html
Infected Technology	Facebook
Recommendation	Change the credential of infected Facebook accounts.

Tailscale VPN nodes vulnerable to DNS rebinding, RCE

Description
An open source mesh virtual private network (VPN) program called Tailscale contains a number of bugs that could let attackers launch remote code execution (RCE) attacks on VPN nodes. Tailscale is reliant on numerous services. The joining of nodes and sending and receiving of packets are handled by the main process, known as tailscaled. To configure and keep track of the services, there is a separate process that offers a user interface and a tray icon. Through an HTTP API named LocalAPI, this front-end interface interfaces with the tailscaled service. The attacker can map their malicious domain to the local IP and issue any commands to the LocalAPI if they are successful in performing a DNS rebinding attack on the Tailscale node. Apart from confirming that client queries originate from the same person executing the Tailscale GUI, the LocalAPI does not authenticate client requests. The malicious website can exploit this feature to change the Tailscale "control plane" to an arbitrary server. The "control plane" is the server that stores the public keys of the VPN nodes (also called the tailnet). The issues have been solved in the latest version of Tailscale. Since Tailscale does not automatically update itself, users should make sure they are running v1.32.3 or later.

Source	https://portswigger.net/daily-swig/tailscale-vpn-nodes-vulnerable-to-dns-rebinding-rce
Infected Technology	Tailscale VPN
Recommendation	Manually update the Tailscale VPN to v1.32.3 or later.

Irish data protection commission (DPC) fined Meta for not protecting Facebook's users' data from scraping	
Description	
Due to the data leak that Facebook experienced in 2021 that exposed the personal information of millions of Facebook users, Meta has been fined €265 million ($275.5 million) by the Irish data protection authority (DPC). Over 32 million records belonged to users from the US, 11 from the UK, and 6 million from India, and the data of Facebook users from 106 countries was freely accessible. Facebook IDs, Phone numbers, full names, birthdates, addresses, biographies, and, for some accounts, the corresponding email addresses, are among the user information that has been exposed. The Irish DPC opened an investigation into alleged GDPR violations by Meta as soon as reports of the data leak popped up. Threat actors gathered the information by taking advantage of a vulnerability fixed in 2019 that allowed for social network data scraping. Now, DPC has concluded the investigation and asserted that Meta violated the GDPR by failing to implement adequate technological and organizational safeguards and failing to implement the essential safeguards required by the European Regulation.	
Source	https://securityaffairs.co/wordpress/139063/laws-and-regulations/irish-dpc-fines-meta-data-scraping.html
Infected Technology	Meta
Recommendation	Mitigation can be installing third party app to detect spam call.

Cisco ISE vulnerabilities can be chained in One-Click exploit

Description	
Multiple vulnerabilities in CISCO identity Service Engine (ISE) could allow remote attacker to inject arbitrary commands, bypass existing security protections, or perform cross-site scripting (XSS) attacks. A total of four vulnerabilities have been identified by a researcher in ISE, the exploitation of all requiring an attacker to be a valid and authorized user of ISE system, The most severe of those vulnerabilities is cve-2022-20964, a command injection bug in ISE's web-based management interface tcpdump feature. Tracked as CVE-2022-20965, another bug is described as an access bypass in web-based management interface. The remaining security defects- CVE-2022-20966 and CVE-2022-20967 could lead to XSS attacks.	
Source	https://www.securityweek.com/cisco-ise-vulnerabilities-can-be-chained-one-click-exploit?&web_view=true
Infected Technology	Cisco Identity Service Engine
Recommendation	• Update to the latest version of the system as soon as patch releases, • Monitor the vulnerability for any exploitation attempt.
CVE_ID	CVE-2022-20964 CVE-2022-20965 CVE-2022-20966 CVE-2022-20967

CISA Warns of Actively Exploited Critical Oracle Fusion Middleware Vulnerability	
Description	
On Monday, the United States Cybersecurity, and Infrastructure Security Agency (CISA) added a critical flaw affecting Oracle Fusion Middleware to its Known Exploited Vulnerabilities (KEV) Catalog, citing active exploitation. The CVE-2021-35587 vulnerability has a CVSS score of 9.8 and affects Oracle Access Manager (OAM) versions 11.1.2.3.0, 12.2.1.3.0, and 12.2.1.4.0. Successful exploitation of the remote command execution bug could enable an unauthenticated attacker with network access to completely compromise and take over Access Manager instances.	
Source	https://thehackernews.com/2022/11/cisa-warns-of-actively-exploited.html
Infected Technology	Oracle Fusion Middleware
Recommendation	It is recommended to apply the vendor patches by December 19, 2022
CVE_ID	CVE-2021-35587

For any queries/recommendations:
Contact us: **whois@cryptogennepal.com**

OUR SERVICES

Our services as information security company includes:


INFORMATION SECURITY AUDIT


VULNERABILITY ASSESSMENT


PENETRATION TESTING


MANAGED/CO.MANAGED SOC


INCIDENT RESPONSE


THREAT ANALYSIS


SERVER HARDENING


CYBER SECURITY CONSULTANT


INFORMATION SECURITY TRAINING

CryptoGen Nepal

https://www.facebook.com/CryptoGenNepal/
https://twitter.com/CryptoGenNepal
https://www.instagram.com/CryptoGenNepal/