November 28, 2022

INFOSEC WEEKLY

#MADE4SECURITY

- ViperSoftX malware installs malicious browser extensions to steal users' passwords and cryptos.
- Update Chrome Browser Now to Patch New Actively Exploited Zero-Day Flaw
- Mastodon vulnerable to multiple system configuration problems
- Leaked Algolia API Keys Exposed Data of Millions of Users
- PoC Code Published for High-Severity macOS Sandbox Escape Vulnerability

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.

ViperSoftX malware installs malicious browser extensions to steal users' passwords and cryptos.

Description	
A windows information stealer named ViperSoftX is a malicious extension for Chromium-based web browser. Because of its standalone features, it enables to track websites visits, steal login credentials and clipboard contents and even swap cryptocurrency addresses via an adversary-in-the-middle (AiTM) attack. Back in 2020, ViperSoftX was a JavaScript-based remote access trojan and cryptocurrency stealer. The objective of the malware is to gather information acting as an extension of chromium-based browser. It also runs arbitrary external payloads and executing commands on the victim's machine. It is primarily distributed from cracked versions of Microsoft Office and Adobe Illustrator through file-sharing websites as the vector for spreading ViperSoftX. In addition to a clean version of the cracked program, the downloaded executable file also contains auxiliary files that enable persistence on the host and include the ViperSoftX PowerShell script.	
Source	https://thehackernews.com/2022/11/this-malware-installs-malicious-browser.html
Infected Technology	Chromium-based Web Browsers
Recommendation	• Never install untrusted Chrome Extensions that are not available in the Web Extension Store. • Do not install cracked software.

Update Chrome Browser Now to Patch New Actively Exploited Zero-Day Flaw

Description	
The high severity vulnerability, identified as CVE-2022-4135, has been reported as a heap buffer overflow in the GPU component. On November 22, 2022, Clement Lecigne of Google's Threat Analysis Group (TAG) is credited with discovering the vulnerability. Threat actors may use heap-based buffer overflow flaws as weapons to execute arbitrary code or crash a computer, resulting in undesirable behavior. To prevent potential threats, users are advised to update to version 107.0.5304.121 for macOS and Linux and 107.0.5304.121/.122 for Windows. As soon as the patches become available, users of Chromium-based browsers including Microsoft Edge, Brave, Opera, and Vivaldi are urged to install updates.	
Source	https://thehackernews.com/2022/11/update-chrome-browser-now-to-patch-new.html
Infected Technology	Chromium-based browsers
Recommendation	• Update Chrome Browser immediately to version 107.0.5304.121 for macOS and Linux and 107.0.5304.121/.122 for Windows • Users using Chromium-based browsers including Microsoft Edge, Brave, Opera and Vivaldi are urged to install patches as soon as they become available.
CVE	CVE-2022-4135

Mastodon vulnerable to multiple system configuration problems

Description	
Multiple instances of social media network Mastodon are vulnerable to system configuration flaws, security researcher Lenin Alevski warns. Security researcher Lenin Alevski found that the infosec. exchange instance of Mastodon was uploaded to storage buckets that failed to impose access controls. This made it possible for an attacker to access a user's profile image or any other submitted data and replace it with arbitrary material. It also meant it was possible to download files from the server – even those shared via direct message (DMs on Mastodon exclude encryption) (DMs on Mastodon omit encryption).	
Source	https://portswigger.net/daily-swig/mastodon-vulnerable-to-multiple-system-configuration-problems
Infected Technology	Mastodon
Recommendation	• Developing a repeatable patching schedule • Keeping software up to date • Disabling default accounts

Leaked Algolia API Keys Exposed Data of Millions of Users

Description	
Threat detection firm CloudSEK has found hundreds of applications exposing Algolia API keys and tens of applications with hardcoded admin secrets, which might allow attackers to steal the data of millions of users. Organizations may leverage Algolia's API to include in their app's capabilities such as search, discovery, and recommendations. The API is utilized by over 11,000 organizations, including Lacoste, Slack, Medium, and Zendesk. CloudSEK claims to have discovered 1,550 applications that exposed Algolia API keys, including 32 apps with hardcoded admin secrets, giving attackers access to pre-defined Algolia API credentials. The 32 guilty applications, CloudSEK states, have more than 2.5 million downloads, potentially exposing the data of their users to unwanted assaults. A threat actor might exploit these holes to read user information, including IP addresses, access details, and analytics data, and delete user information.	
Source	https://www.securityweek.com/leaked-algolia-api-keys-exposed-data-millions-users
Infected Technology	Algolia API
Recommendation	Changed the infected API credentials.

PoC Code Published for High-Severity macOS Sandbox Escape Vulnerability

Description	
A security researcher has published details and proof-of-concept (PoC) code for a macOS vulnerability that could be exploited to escape a sandbox and execute code within Terminal. Tracked as CVE-2022-26696 (CVSS score of 7.8), the security defect was identified and reported last year, with a patch available since the release of macOS Monterey 12.4 in May. In its advisory, Apple notes that the flaw allowed a sandboxed process to circumvent sandbox restrictions, and that improved environment sanitization resolved the issue.Successful exploitation of the vulnerability would require for the attacker to be able to execute low-privileged code on the target system.	
Source	https://www.securityweek.com/poc-code-published-high-severity-macos-sandbox-escape-vulnerability
Infected Technology	Apple macOS terminal
Recommendation	Update to the latest version of the system as soon as possible.
CVE_ID	CVE-2022-26696

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/CryptoGenNepa