October 10, 2022

INFOSEC WEEKLY

#MADE4SECURITY

- LofyGang Distributed 200 Malicious NPM Packages to Steal Credit Card Data
- Hackers Exploiting Unpatched RCE Flaw in Zimbra Collaboration Suite
- Details Released for Recently Patched new macOS Archive Utility Vulnerability
- Facebook Detects 400 Android and iOS Apps Stealing Users Log-in Credentials.
- JavaScript sandbox vm2 contains RCE risks

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.

LofyGang Distributed 200 Malicious NPM Packages to Steal Credit Card Data

Description

Multiple campaigns that distributed trojanized and typosquatted packages on the NPM open-source repository have been identified as the work of a single threat actor dubbed LofyGang. Checkmarx said it discovered 199 rogue packages totaling thousands of installations, with the group operating for over a year with the goal of stealing credit card data as well as user accounts associated with Discord Nitro, gaming, and streaming services. Various pieces of the attack puzzle have already been reported by JFrog, Sonatype, and Kaspersky (which called it LofyLife), but the latest analysis pulls the various operations together under one organizational umbrella that Checkmarx is referring to as LofyGang. Believed to be an organized crime group of Brazilian origin, the attackers have a track record of using sock puppet accounts to advertise their tools and services on GitHub, YouTube, and leaking thousands of Disney+ and Minecraft accounts on underground hacking forums.

Source	https://thehackernews.com/2022/10/lofygang-distributed-200-malicious-npm.html?m=1
Infected Technology	• Discord • Repl.it • glitch • GitHub • Heroku
Recommendation	Do not Install unauthorized apps and software.
CVE_ID	N/A

Hackers Exploiting Unpatched RCE Flaw in Zimbra Collaboration Suite

Description

Zimbra's enterprise collaboration software and email platform include a serious remote code execution vulnerability that is now being aggressively exploited giving attackers a means to upload arbitrary files to target installations and perform malicious operations. The flaw affects numerous Linux distributions, including Oracle Linux 8 and Red Hat Enterprise Linux 8, and is present in versions 8.8.15 and 9.0 of the programs. An attacker must send a CPIO or TAR archive file to a server that is vulnerable to exploit the bug successfully. Amavis will then analyze the file and extract its contents using the cpio file archiver software. The attacker can write to any location on the file system that the Zimbra user can access because cpio lacks a mode that allows it to be used securely on untrusted files.

Source	https://thehackernews.com/2022/10/hackers-exploiting-unpatched-rce-flaw.html?m=1
Infected Technology	Zimbra collaboration software
Recommendation	• Patches are expected to be released soon.
CVE_ID	CVE-2022-41352

Details Released for Recently Patched new macOS Archive Utility Vulnerability

Description	
The details about a security flaw in Apple's macOS operating system have been shared by a security researcher that could potentially be exploited to run malicious applications in a manner that can bypass Apple's security measures. The vulnerability is rooted in the built-in Archive Utility and could lead to the execution of an unsigned and unnotarized application without displaying security prompts to the user, by using a specially crafted archive. The vulnerability is described as a logic issue that allows an archive file to get around Gatekeeper checks.	
Source	https://thehackernews.com/2022/10/details-released-for-recently-patched.html?m=1
Infected Technology	macOS
Recommendation	• Update to latest version
CVE_ID	CVE-2022-32910

Facebook Detects 400 Android and iOS Apps Stealing Users Log-in Credentials.

Description
Meta Platforms on Friday disclosed that it had identified over 400 malicious apps on Android and iOS that it said targeted online users with the goal of stealing their Facebook login information. These apps were listed on the Google Play Store and Apple's App Store and disguised as photo editors, games, VPN services, business apps, and other utilities to trick people into downloading them. 42.6% of the rogue apps were photo editors, followed by business utilities (15.4%), phone utilities (14.1%), games (11.7%), VPNs (11.7%), and lifestyle apps (4.4%). Interestingly, a majority of the iOS apps posed as ads manager tools for Meta and its Facebook subsidiary. The apps ultimately functioned as a means to steal the credentials entered by users by displaying a "Login With Facebook" prompt. All the apps in question have been taken down from both app stores. The list of 402 apps (355 Android and 47 iOS apps)

Source	https://thehackernews.com/2022/10/facebook-detects-400-android-and-ios.html?m=1
Infected Technology	Facebook Login Credentials.
Recommendation	• Do not Install unauthorized apps and software.
CVE_ID	N/A

<table>
<tr><td colspan="2">JavaScript sandbox vm2 contains RCE risks</td></tr>
<tr><td colspan="2">Description</td></tr>
<tr><td colspan="2">To conduct remote code execution (RCE) on the host device, bad actors may be able to get through the sandbox's security measures thanks to a flaw in the popular JavaScript sandbox environment vm2. With more than four million downloads each week, Vm2 enables Node.js servers to run untrusted code in a secure context without jeopardizing the server's security. Because vm2 is utilized in both development and production environments, the vulnerability—which was assigned a maximum CVSS score of 10—has a greater potential impact. This channel allows the attacker to run arbitrary code on the Node.js server, including invoking functions that run system commands.</td></tr>
<tr><td>Source</td><td>https://portswigger.net/daily-swig/javascript-sandbox-vm2-remediates-remote-code-execution-risk</td></tr>
<tr><td>Infected Technology</td><td>JavaScript sandbox vm2</td></tr>
<tr><td>Recommendation</td><td>Upgrade to latest version of vm2</td></tr>
</table>

Nepxion Discovery software with Spring Cloud functionality fails to patch RCE vulnerability.

Description

Nepxion Discovery, an open-source project that offers functionality for the Spring Cloud framework, contains an unpatched remote code execution (RCE) vulnerability. On September 9, information about the vulnerability and another information disclosure bug in Nepxion Discovery was made public by security researchers from the GitHub Security Lab (GHSL). A firm with a basis in China named Nepxion manages a number of Spring Cloud-related open-source projects. Despite having over 1,300 forks, the Nepxion Discovery GitHub page's security policy page and security advisories tab are both suppressed. The most serious flaw, identified as GHSL-2022-033 (CVE-2022-23463), according to GHSL researcher Jorge Rosillo, is a fundamental problem in the discovery-commons function that makes the program susceptible to SpEL Injection. Attacks using SpEL Injection happen when there isn't enough security to prevent user input from going straight to a SpEL expression parser. Two endpoints in this scenario translate user input into expressions, transmit them, and allow input to communicate with Java classes, including java.lang. Runtime, resulting in RCE

Source	https://portswigger.net/daily-swig/javascript-sandbox-vm2-remediates-remote-code-execution-risk
Infected Technology	Nepxion Discovery GitHub page
Recommendation	Stay up to date with patch news from Nexion
CVE_ID	CVE-2022-23464

Improved Mitigation Measures Issued by Microsoft for unpatched Exchange Server Vulnerabilities.

Description

Microsoft issued new workarounds to prevent active exploitations of zero-day flaws in Exchange servers, after it was discovered that their previous recommendations were easily bypassed by hackers. The vulnerabilities, dubbed ProxyNotShell, enable attackers to perform remote code execution against exchange servers with elevated privileges. Currently, it is not clear when Microsoft will issue patches from the vulnerabilities. However, it is anticipated that updates will be pushed as a part of Tuesday updates on October 11, 2022.

Source	https://thehackernews.com/2022/10/microsoft-issues-improved-mitigations.html
Infected Technology	Microsoft Exchange Server
Recommendation	Issue the new mitigation measures and apply official patches as soon as made available.
CVE_ID	CVE-2022-41040, CVE-2022-41082

Fortinet Warns of New Auth Bypass Flaw Affecting FortiGate and FortiProxy

Description	
Fortinet has warned its customers of a security flaw affecting FortiGate firewalls and Forti Proxy web proxies that could potentially allow an attacker to perform unauthorized actions on susceptible devices. Tracked as CVE-2022-40684 (CVSS score: 9.6), the critical flaw relates to an authentication bypass vulnerability that may permit an unauthenticated adversary to carry out arbitrary operations on the administrative interface via a specially crafted HTTP(S) request. Due to the ability to exploit this issue remotely, Fortinet is strongly recommending all customers with the vulnerable versions to perform an immediate upgrade. As temporary workarounds, the company is recommending users to disable internet-facing HTTPS Administration until the upgrades can be put in place, or alternatively, enforce a firewall policy to "local-in traffic."	
Source	https://thehackernews.com/2022/10/fortinet-warns-of-new-auth-bypass-flaw.html
Infected Technology	FortiOS - From 7.0.0 to 7.0.6 and from 7.2.0 to 7.2.1 FortiProxy - From 7.0.0 to 7.0.6 and 7.2.0
Recommendation	• Disable internet-facing HTTPS Administration • Enforce a firewall policy to "local-in traffic”.
CVE_ID	CVE-2022-40684

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/