December 27, 2021

INFOSEC WEEKLY

#MADE4SECURITY

- macOS Bug that could let Malware Bypass Gatekeeper Security
- New Mobile Vulnerabilities Affect All Cellular Generations Since 2G (GSM)
- Over 500,000 Android Users Downloaded a New Joker Malware App from Play Store
- Grim Finance hacked – $30 million worth of tokens stolen
- Unpatched Vulnerabilities disclosed in Microsoft Teams Software

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.

macOS Bug that could let Malware Bypass Gatekeeper Security

Description	
A security vulnerability in Apple's macOS operating system was recently patched, allowing a threat actor to "trivially and reliably" bypass a "myriad of core macOS security features" and run arbitrary code. The security feature guarantee that only trusted apps are executed and that they have passed an automatic procedure known as "app notarization". This vulnerability in Apple's Gatekeeper process allows attackers to craft an application without providing an interpreter (i.e., #!) and still get the underlying operating system to launch the script without raising any alert. Threat actors can exploit this flaw by tricking their targets into opening a rogue app that can be camouflaged as Adobe Flash updates or 'trojan zed' versions of Microsoft Office.apps are executed and that they have passed an automatic procedure known as "app notarization".	
Source	https://thehackernews.com/2021/12/expert-details-macos-bug-that-could-let.html
Infected Technology	macOSmacOS
Recommendation	• Apple has released security updates addressing this issue which is important to apply these updates as soon as possible to prevent vulnerability exploitation.
CVE_ID	CVE-2021-30853

New Mobile Vulnerabilities Affect All Cellular Generations Since 2G (GSM)

Description	
A new critical security weakness has been disclosed by Mozilla and provided fixes to address the vulnerability that could be potentially exploited by an adversary to crash a vulnerable application and even execute arbitrary code. The vulnerability resides s handoff, is a telecommunications procedure that allows a phone conversation or data session to be moved from one cell site (or base station) to another without losing connectivity. Vulnerabilities in the handover method affect all different handover circumstances and scenarios that are reliant on unverified measurement reports and signal strength criteria, according to the research.	
Source	https://thehackernews.com/2021/12/new-mobile-network-vulnerabilities.html
Infected Technology	NSS versions prior to 3.73 or 3.68.1 ESRAll Cellular Generations Since 2G (GSM) (for e.g., OnePlus 6, Apple iPhone 5, Samsung S10 5G, and Huawei Pro P40 5G)NSS versions prior to 3.73 or 3.68.1 ESRAll Cellular Generations Since 2G (GSM) (for e.g., OnePlus 6, Apple iPhone 5, Samsung S10 5G, and Huawei Pro P40 5G)
Recommendation	• Apply 5G Software-defined network updates.

Over 500,000 Android Users Downloaded a New Joker Malware App from Play Store

Description	
A malicious messaging-focused app named “Color Message" with more than 500,000 downloads from the Google Play app store has been found hosting malware that stealthily exfiltrates users' contact lists to an attacker-controlled server and signs up users to unwanted paid premium subscriptions without their knowledge.nwanted paid premium subscriptions without their knowledge.A malicious messaging-focused app named “Color Message" with more than 500,000 downloads from the Google Play app store has been found hosting malware that stealthily exfiltrates users' contact lists to an attacker-controlled server and signs up users to u	
Source	https://thehackernews.com/2021/12/over-500000-android-users-downloaded.html
Infected Technology	Android phones with “Color Message” installed. Android phones with “Color Message” installed.
Recommendation	• Apply 5G Software-defined network updates.

Grim Finance hacked – $30 million worth of tokens stolenGrim Finance hacked – $30 million worth of tokens stolen

Description	
Grim Finance, a DeFi protocol, and Smart Yield Optimizer Platform has announced that the platform was hacked Saturday 18th in an “advanced attack” that allowed hackers to steal over $30 million worth of Fantom Tokens. In a series of tweets, Grim Finance explained that the attack was possible because unknown attackers exploited a flaw in its vault contract. Resultantly, the platform has paused all the vaults to avoid further damage as deposited funds are currently at risk.plained that the attack was possible because unknown attackers exploited a flaw in its vault contract. Resultantly, the platform has paused all the vaults to avoid further damage as deposited funds are currently at risk.Grim Finance, a DeFi protocol, and Smart Yield Optimizer Platform has announced that the platform was hacked Saturday 18th in an “advanced attack” that allowed hackers to steal over $30 million worth of Fantom Tokens. In a series of tweets, Grim Finance ex	
Source	https://www.hackread.com/grim-finance-hacked-30-million-stolen/
Infected Technology	All the vaults and deposited fundsAll the vaults and deposited funds
Recommendation	• Use different and more secure platform to store crypto.

Unpatched Vulnerabilities disclosed in Microsoft Teams Software

Description	
Dces, spoofing the link preview, and leaking IP addresses as well as performing Dos on their Teams app/channels for Android users. Out of the four vulnerabilities, Microsoft has addressed only one that results in IP address leakage of Android devices and noted that a fix for the denial-of-service flaw will be considered in a future version of the product. The chief flaw among all those is a server-side request forgery vulnerability which could be exploited to glean information from Microsoft's local Network.isclosure of the vulnerabilities came from a Berlin-based Cybersecurity firm. It was found that the implementation of the link preview feature was susceptible. The issue was suspected to be several issues that could allow accessing internal Microsoft service	
Source	https://thehackernews.com/2021/12/researchers-disclose-unpatched.html
Infected Technology	Microsoft TeamsMicrosoft Teams
Recommendation	• Do not open suspicious URLs

Telegram Exploited by Attackers to Spread Malware.

Description	
A new critical security weakness has been disclosed by Mozilla and provided fixes to address the vulnerability that could be potentially exploited by an adversary to crash a vulnerable application and even execute arbitrary code. The vulnerability resides ma variety of messaging and file-sharing channels, such as Discord, Edge, FileZilla, OpenVPN, Outlook as well as Telegram itself and along with a variety of cryptocurrency wallets including AtomicWallet, BitcoinCore, ByteCoin, Exodus, Jaxx and Monero. Attackers had been using the handle “Smokes Night” to disseminate Echelon although the successfulness is yet unknown. Telegram messaging Platform has undoubtedly become a hotspot of activity for hackers who’ve already taken advantage of its popularity and large attack surface by distributing malware on the network via bots, rogue accounts and other methods.	
Source	https://www.cysecurity.news/2021/12/telegram-exploited-by-attackers-to.html?utm_source=dlvr.it&utm_medium=twitter&m=1
Infected Technology	NSS versions prior to 3.73 or 3.68.1 ESRTelegram Messaging PlatformNSS versions prior to 3.73 or 3.68.1 ESR Telegram Messaging Platform
Recommendation	• Be aware when chaining channels in Telegram

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/