January 10, 2022

INFOSEC WEEKLY

#MADE4SECURITY

- Attackers Exploit Flaw in Google Doc's Commen Feature
- Apple iPhone Malware Tactic Causes Fake Shutdowns to Enable Spying
- VMware Patches Important Bug Affecting ESXi Workstation, and Fusion Products
- Attackers Exploiting Drop ZLoader
- Honda Y2K22 Navigation System Clock Bug Migh Not be Fixed Until August
- Privilege escalation vulnerability in Google Android TV

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.

Attackers Exploit Flaw in Google Doc's Comment Feature

Description	
Google Doc's comment function has been used by "a new, enormous wave of hackers", to send malicious links in a phishing campaign mainly targeting Outlook users. The threat actors mention the targeted user with an "@" which automatically sends an email to that person's inbox. The vulnerability has been identified but so far Google has not responded to the issue.	
Source	https://threatpost.com/attackers-exploit-flaw-google-docs-comments/177412/
Infected Technology	Google Docs
Recommendation	Reach out to the legitimate sender and confirm they meant to send that. Maintain a standard "cyber hygiene" when reviewing comments.

Apple iPhone Malware Tactic Causes Fake Shutdowns to Enable Spying

Description	
A new iPhone technique may hijack and block any user-initiated shut-down, imitating a legitimate power-off while malware remains running in the background. Because an infected person may believe "that the phone has been shut down, while in reality, it is still functioning," researchers stated, the method provides a great cover for harmful activities. "The NoReboot method imitates a complete shutdown." The user is unable to distinguish between a genuine and a false shutdown. Until the user switches the phone back 'on,' there is no user interface or button feedback.	
Source	https://threatpost.com/apple-iphone-malware-fake-shutdowns-spying/177420/
Infected Technology	Every Version of iPhones
Recommendation	Maintain and follow apple's latest update timely. Take the usual vetting precautions when downloading and installing new apps.

VMware Patches Important Bug Affecting ESXi, Workstation, and Fusion Products

Description	
The "critical" security vulnerability that may be exploited by a threat actor to take control of impacted computers has been patched by VMware in Workstation, Fusion, and ESXi. Using this vulnerability in combination with other flaws, a malicious actor with access to a virtual machine with CD-ROM device emulation may be able to execute the malware on the hypervisor from a virtual machine.	
Source	https://thehackernews.com/2022/01/vmware-patches-important-bug-affecting.html
Infected Technology	ESXi versions 6.5, 6.7, and 7.0; Workstation versions 16.x; and Fusion versions 12.x
Recommendation	Stop every CD-ROM/DVD drive on all active virtual machines to avoid any possible exploitation. Install latest patched updates.
CVE_ID	CVE-2021-22045

Attackers Exploiting Drop ZLoader

Description	
Hackers are exploiting a known vulnerability in Microsoft's code signing process to install ZLoader malware. The campaign was discovered for the first time in November 2021. It gains initial access to the machine by using legitimate remote monitoring and management software and then installs the malware using a modified dynamic link library (DLL) file. In 2013, Microsoft issued a patch for the Authenticode vulnerability in its code-signing process. The repair was supposed to be rolled out to all customers, but Microsoft opted to make it optional due to the possibility of a large number of false positives.	
Source	https://virtualattacks.com/news/hackers-exploiting-microsoft-signature-verification-to-drop-zloader-malware/
Infected Technology	Microsoft's e-signature verification tool
Recommendation	Install latest patched updates.
CVE_ID	CVE-2013-3900

Honda Y2K22 Navigation System Clock Bug Might Not be Fixed Until August

Description	
On January 1, 2022, a bug in the navigation system clocks in some Honda and Acura vehicles caused the clocks to reset to 2002. The problem appears to affect vehicles manufactured between 2004 and 2012. The fault would not be repaired until August, according to several vehicle owners. Software development must take into account the length of time a system is expected to be operational, as well as the complete life cycle. As more "smart" features are added to cars, it's crucial to remember that, unlike smartphones, cars are designed to last for 10 years or more.	
Source	https://www.theverge.com/2022/1/8/22873403/honda-acuras-y2k22-bug-clocks-reset-2002
Infected Technology	Some Honda and Acura Models
Recommendation	Install latest patched updates.

Privilege escalation vulnerability in Google Android TV

Description	
The pairing process on Android TV lacks a rate limiter which makes a silent pairing possible. Local privilege escalation is possible due to a use-after-free vulnerability in the kernel. As a consequence of a "write-what-where" situation, a threat actor may be able to access or reference memory after it has been released, resulting in the execution of arbitrary code to acquire control over a victim's system.	
Source	https://thehackernews.com/2021/11/google-warns-of-new-android-0-day.html
Infected Technology	Android TV
Recommendation	Update to latest available patch.
CVE_ID	CVE-2021-0889

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/