October 25, 2021

INFOSEC WEEKLY

#MADE4SECURITY

- Campaign using YouTube to push malware to steal passswords
- Rootkit abusing Microsoft Issued Digital certificate
- Google Chrome Patches 19 vulnerability
- Side-Channel Attack Targeting AMD CPUs
- Oracle Critical Patch Update

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.

Campaign using YouTube to push malware to steal passswords

Description	
Threat actors are using YouTube to spread malware that steals saved password. The distributed malware is a Trojan that steals password, screenshot of windows, cookies, credit cards information saved in browsers along with arbitrary files in the system. The trojan is distributed embedded link in the video description of thousands of videos and channels. Threat actors are creating 100 new videos and 81 new channels in twenty minutes. The Google account stole through the process is used to create channel and is added to the campaign.	
Source	https://blog.google/threat-analysis-group/phishing-campaign-targets-youtube-creators-cookie-theft-malware/
Infected Technology	Social Engineering
Recommendation	Do not download software from untrusted sources

Rootkit abusing Microsoft Issued Digital certificate

Description	
Researchers from BitDefender has identified a rootkit, named FiveSys, that is using Microsoft-Issued Digital certificate to evade detection. FiveSys has been affecting devices for more than a year and is currently targeted toward China. The malware is using proxy to route its traffic to its command center from a list of 300 randomly generated domain name that are encrypted to protect takedown attempts. Microsoft has now revoked the signature of FiveSys after abuse has been reported.	
Source	https://www.bitdefender.com/files/News/CaseStudies/study/405/Bitdefender-DT-Whitepaper-Fivesys-creat5699-en-EN.pdf
Infected Technology	Microsoft Windows
Recommendation	Do not download files from untrusted sources Review running services Use endpoint protection services

Google Chrome Patches 19 vulnerability

Description	
Google has released a new version for Chrome that patches 19 vulnerabilities out of which 5 were rated High impact bugs. The high severity vulnerabilities were buffer overflow and user after free in incognito, dev tools, PDFium and V8 engine which were all reported by external researchers. The technical details of all vulnerabilities are not yet disclosed to allow user to update the patch.	
Source	https://chromereleases.googleblog.com/2021/10/stable-channel-update-for-desktop_19.html
Infected Technology	Google Chrome 94
Recommendation	Update the browser to Chrome 95
CVE	CVE-2021-37981, CVE-2021-37982, CVE-2021-37983, CVE-2021-37984, CVE-2021-37985, CVE-2021-37986, CVE-2021-37987, CVE-2021-37988, CVE-2021-37989, CVE-2021-37990, CVE-2021-37991, CVE-2021-37992, CVE-2021-37993, CVE-2021-37996, CVE-2021-37994, CVE-2021-37995

Side-Channel Attack Targeting AMD CPUs

Description	
Researchers have identified a new side-channel attack vulnerability that affects all AMD processors. The vulnerability allows application being installed in the system to collect sensitive information from memory associated to other application such as password and encryption keys. No mitigation steps has been provided with statement that this vulnerability, “do not directly leak data across address space boundaries”	
Source	https://cispa.de/en/research/publications/3507-amd-prefetch-attacks-through-power-and-time
Infected Technology	AMD CPU
CVE	CVE-2021-26318

Oracle Critical Patch Update

Description	
Oracle has released Critical Patch Update, which contains 419 security patches for vulnerabilities across the company's entire portfolio. Sixty-six of the 419 new security fixes in the CPU address significant vulnerabilities, one of which has a CVSS score of ten. In addition, the CPU addresses 60 vulnerabilities with a CVSS score of 8 to 9. With 71 patches, Oracle Communications received the most in this CPU. Sixty-six of these flaws might be exploited remotely without requiring authentication.	
Source	https://www.oracle.com/security-alerts/cpuoct2021.html
Infected Technology	Oracle Products.
Recommendation	Update the latest available patches

PoC Exploit Released for macOS GateKeeper Bypass

Description	
The proof-of-concept exploit targets a flaw that can allow all three of Apple's anti-malware safeguards, notably file quarantine, Gatekeeper, and notarization, to be bypassed. This flaw was discovered in macOS Big Sur and Catalina's Archive Utility component and can be exploited with a specially designed ZIP file. To carry out a successful exploitation, the attacker must persuade the victim to download and open the archive to run the malicious code contained within. An attacker might leverage the vulnerability to execute unsigned binaries on macOS devices, even if Gatekeeper was enforcing code signatures and the user was not notified of the malicious code execution.	
Source	https://labs.f-secure.com/blog/the-discovery-of-cve-2021-1810/
Infected Technology	macOS
Recommendation	Update the latest available patch
CVE-ID	CVE-2021-1810

Multiple Vulnerabilities in ZTE LTE Router

Description	
Cisco Talos has disclosed multiple vulnerabilities in ZTE MF971R LTE router. The router uses GSM to provide Wi-Fi connection as a portable device. The device is vulnerable to stack overflow vulnerabilities that allowed attacker to execute remote code in vulnerable device. The device is vulnerable to cross site scripting that allows threat actor to execute malicious JavaScript payload on victim's browser. The router is also vulnerable to configuration file overwrite and CRLF injection. The OEM has acknowledged and released update for affected devices.	
Source	https://blog.talosintelligence.com/2021/10/vuln-spotlight-.html?&web_view=true
Infected Technology	ZTE MF971R LTE router
Recommendation	Upgrade router firmware
CVE-ID	

Multiple malicious packages disguised as JavaScript Libraries

Description	
Researchers have uncovered multiple malicious packages disguised as legitimate JavaScript Libraries on npm registries. These packages are dubbed okhsa, klow and klown and launch cryptominers on Windows, macOS and Linux machines.	
Source	https://blog.sonatype.com/newly-found-npm-malware-mines-cryptocurrency-on-windows-linux-macos-devices
Infected Technology	Windows, macOS, Linux
Recommendation	The packages have been taken down by the npm security team

WinRAR Bug

Description	
WinRAR trial ware, a file archiver windows utility has been deemed vulnerable as a bug has been discovered that can be abused by a remote perpetrator to execute arbitrary code on victims' system It allows request interception and modification sent to the user's application.	
Source	https://thehackernews.com/2021/10/bug-in-free-winrar-software-could-let.html
Infected Technology	WinRAR trialware 5.70
Recommendation	Upgrade to WinRAR version 6.02
CVE-ID	CVE-2021-35052

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/