June 13, 2020

INFOSEC WEEKLY

#MADE4SECURITY

- Joker Malware once again Bypass Google Security
- Citrix issues critical patches Affecting Multiple products
- Advertising plugins for Word Press Threatens Full Site Take over
- Business giant Xerox allegedly suffers Maze Ransomware attack
- NVIDIA fixes Code execution vulnerability in GeForce experience
- POS Malware leverage DNS for secret Communication
- New Zero –Day Vulnerability in Zoom For Windows 7
- Critical Flaws on Common home routers

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, Trip Advisor, 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.

1. Joker Malware once again Bypass Google Security

Description	
Billing fraud malware Joker evades Google Play security to infect Android devices. Hidden in legitimate applications, it has targeted Android users to subscribe them to premium services without their consent. It's a tricky new variant of the joker Malware, identified by researchers with security firm. To go undetected, the malware hid its malicious payload inside the metadata of Android Manifest File. Then the malicious code was stored in base64 -encoded strings. The malicious payload would remain dormant, while Google was evaluating the apps. Once the app is approved the developers starts loading the malicious payload.	
Source	https://research.checkpoint.com/2020/new-joker-variant-hits-google-play-with-an-old-trick/
Infected Technology	
Recommendation	• Check billing statement for unauthorized charges • Uninstall the infected Apps from your android device • Install a security solution to prevent future infections • Make sure to scrutinize your permissions for every app installed on your Android device.

2. Citrix issues critical patches Affecting Multiple products

Description	
Citrix issued new security patches for as many as 11 security flaws that affect it's networking products – Citrix Application Delivery Controller (ADC), Citrix Gateway, and SD-WAN WAN Optimization edition (WANOP). Out of 11 vulnerabilities, there are six possible attacks routes; five of those have barriers to prevent exploitation. Three of six possible attacks in CTX276688 happen in the management interface of a vulnerable device. Two of the remaining three possible attacks would require a malicious actor to gain access to a target device and conduct an attack. Threat actors could also mount attacks on Virtual IPs (VIPs). VIPs, among other things, are used to provide users with a unique IP address for communicating with network resources for applications that do not allow multiple connections or users from the same IP address.	
Source	https://www.citrix.com/blogs/2020/07/07/citrix-provides-context-on-security-bulletin-ctx276688/
Infected Technology	Citrix ADC, Gateway, SD-WAN WANOP Appliances (4000-WO, 4100-WO,5000-WO and 5100-WO.)
CVEs	CVE-2019-18177, CVE-2020-8187, CVE-2020-8190, CVE-2020-8191, CVE-2020-8193, CVE-2020-8194, CVE-2020-8195, CVE-2020-8196, CVE-2020-8197, CVE-2020-81978, CVE-2020-8199
Recommendation	Download And apply latest builds for Citrix ADC, Citrix Gateway, Citrix SD-WAN WANOP appliances as soon as possible

3. Advertising plugins for Word Press Threatens Full Site Take over

Description	
The Adning Advertising plugin for WordPress, a premium plugin with over 8,000 customers, contains a critical remote code-execution vulnerability with the potential to be exploited by unauthenticated attackers. The plugin's author, Tunafish, has rolled out a patched version (v.1.5.6), which site owners should update to as soon as possible. The bug could allow complete site takeover. it has already been the subject of in-the-wild attacks, according to an analysis from Wordfence issued on Wednesday. That said, the firm said the attacks so far have been limited in scope and scale.	
Source	https://threatpost.com/advertising-plugin-wordpress-full-site-takeovers/157283/?web_view=true
Infected Platform	Word Press Plugin
Recommendation	Update the latest patch available

4. Business giant Xerox allegedly suffers Maze Ransomware attack

Description	
The maze ransomware operators have posted a set of 10 screenshots of the Xerox corporation, which clearly affirms that the maze ransomware operators have hacked Xerox corporation. According to the data that has been posted by the maze operators, they have carried out this operation on 25 June 2020. The maze operators have encrypted multiple compromised files of the Xerox corporation. the Maze ransomware operators demanded to have taken more than 100GB of files from Xerox corporation, and therefore they are threatening the company that they will publish the encrypted data if they don't pay the ransom.	
Source	https://www.bleepingcomputer.com/news/security/business-giant-xerox-allegedly-suffers-maze-ransomware-attack/
Infected Technology	Xerox
Recommendation	• Always prefer a secure and robust password. • Always keep activated the multi-factor authentication security system. • Keep a regular check up on your financial transactions. • Always keep your PC up to date.

5. NVIDIA fixes Code execution vulnerability in GeForce experience

Description	
NVIDIA has addressed a vulnerability in the Windows NVIDIA GeForce Experience (GFE) software that could allow local attackers to execute arbitrary code, trigger a denial of service (DoS) state, or access privileged information on unpatched systems. Even though the security flaw tracked as CVE-2020-5964 requires attackers to have local user access to the device and cannot be exploited remotely, it can still be abused with the help of malicious tools delivered to systems running vulnerable NVIDIA GFE versions. After successfully exploiting the vulnerability, the flaw could enable attackers could execute arbitrary code on Windows machines running unpatched NVIDIA GFE software versions. They could also gain access to sensitive information beyond the permissions initially granted by the compromised system or render them unusable by triggering a denial of service state.	
Source	https://www.zdnet.com/article/nvidia-fixes-code-execution-vulnerability-in-geforce-experience/?&web_view=true
Infected Technology	NVIDIA GeForce Experience Version before 3.20.4
Recommendation	Update the latest patch by NVIDIA
CVEs	CVE-2020-5964

6. POS Malware leverage DNS for secret Communication

Description	
Attackers often tend to hide their malicious communications via innovative techniques, to dodge the detection by security solutions. One such attempt was recently made by a Point of Sale (POS)-targeting malware, that targeted DNS for its communications. In June, Alina POS Malware was found using the DNS protocol to send the stolen credit card details to the attacker's remote servers. On the POS devices, the malware performs RAM scrapping to find and steal any unencrypted credit card related information. Before sending the card details to C2 servers, the malware validates the card numbers by using Luhn checksum algorithm. In February, the Mozart Malware was found using the DNS protocol (DNS TXT records) for communication with the remote attackers, to avoid detection by security software.	
Source	https://cyware.com/news/pos-malware-leverages-dns-for-secret-communications-49a90b99

7. New Zero –Day Vulnerability in Zoom For Windows 7

Description	
A zero-day vulnerability has been discovered in Zoom video conferencing software for Windows that could allow an attacker to execute arbitrary code on a victim's computer running Microsoft Windows 7 or older. The vulnerability has been discovered by a researcher who reported it to Acros Security, who then reported the flaw to the Zoom security team earlier today. The researcher wishes to remain anonymous. Researchers at Acros Security have also developed a working proof-of-concept exploit for the vulnerability, which they have shared with Zoom and will not release until the company fixes the issue.	
Source	https://blog.opatch.com/2020/07/remote-code-execution-vulnerability-in.html
Infected Technology	Zoom Video Conferencing Application
Recommendation	Apply available micropatches

8. Critical Flaws on Common home routers

Description	
Researchers found 127 popular home routers with at least one critical security flaw. The list of devices known to possess major cyber security vulnerabilities includes, D-Link, Netgear, ASUS, Linksys, TP-Link and Zyxel. Researchers examined the routers based on several key aspects: device updates, version of operating system and any known critical vulnerabilities affecting them; exploit mitigation techniques by vendors and how often they activate them; the existence of private cryptographic key material in the router's firmware; and the existence of hard-coded login credentials. Providing hard-coded credentials is an especially vulnerable situation for a device, as evidenced by the destructive Mirai botnet, which used hard-coded telnet credentials to infect millions of embedded devices, researchers noted.	
Source	https://www.fkie.fraunhofer.de/content/dam/fkie/de/documents/HomeRouter/HomeRouterSecurity_2020_Bericht.pdf
Infected Technology	Multiple Home routers
Recommendation	Update home routers to the latest firmware released by respective vendors

For any queries/recommendations:
Contact us: **whois@cryptogennepal.com**