October 26, 2020

INFOSEC WEEKLY

#MADE4SECURITY

- Attackers prey on Microsoft Teams accounts to steal credentials
- NVIDIA Patches GeForce Experience Vulnerabilities
- Chrome Zero-day Under Active Attacks
- Unauthenticated RCE on MobileIron MDM
- Multiple Address bar spoofing vulnerabilities

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.

1. Attackers prey on Microsoft Teams accounts to steal credentials

Description
Microsoft Teams is a popular communication tool, particularly during the pandemic, making it an attractive brand for attackers to impersonate. This attack impersonates an automated message from Microsoft Teams in order to steal recipient's login credentials. A new phishing attack that impersonates an automated communication message from Microsoft Teams, and tries to get you to click a link to take you to the Teams web interface, where you supply your username and password. The page looks just like Microsoft's login page. One of the URLs that has been seen when clicked thru is Microsoft Teams which is close enough to fool the brain if you are not paying attention. These phishing emails may also be disguised as coming from coworkers which can be easily accomplished by automatically scraping public info from social media sites like LinkedIn.

Source	https://abnormalsecurity.com/blog/microsoft-teams-impersonation/
Infected Technology	Microsoft Teams
Recommendation	• Be cautious on hovering the links and of phishing mails. • Do not provide sensitive information by clicking links included in Emails

2. NVIDIA Patches GeForce Experience Vulnerabilities

Description

NVIDIA released a security update for the Windows NVIDIA GeForce Experience (GFE) app to address vulnerabilities that could enable attackers to execute arbitrary code, escalate privileges, gain access to sensitive info, or trigger a denial of service (DoS) state on systems running unpatched software. While these flaws require attackers to have local user access and cannot be exploited remotely, they can still be abused using malicious tools deployed on systems running vulnerable NVIDIA GFE versions. Additionally, attacks that would exploit these bugs are of low complexity according to NVIDIA, while also requiring low privileges, and need no user interaction.

Source	https://nvidia.custhelp.com/app/answers/detail/a_id/5076/kw/security%20bulletin
Infected Technology	NVIDIA GeForce Experience
CVE	CVE-2020-5977, CVE-2020-5990, CVE-2020-5978
Recommendation	Updates the patch available

3. Chrome Zero-day Under Active Attacks

Description

Security research of Google project Zero discovered which is classified as a type of memory-corruption flaw called a heap buffer overflow in Free Type. Google releasee Chrome version 86.0.4240.111 today to patch several security high-severity issues, including a zero-day vulnerability that has been exploited in the wild by attackers to hijack targeted computers. The actively exploited vulnerability is a type of memory-corruption flaw called heap buffer overflow in Freetype, a popular open source software development library for rendering fonts that comes packaged with Chrome.

Source	https://chromereleases.googleblog.com/2020/10/stable-channel-update-for-desktop_20.html
Infected Technology	Chrome, FreeType Font Library
CVE_ID	CVE-2020-15999
Recommendation	• Update the chrome browser

4. Unauthenticated RCE on MobileIron MDM

Description	
MobileIron's Enterprise Mobile Device Management (MDM), a solution used to manage fleets of mobile devices, is under attack by cybercriminals. Recently, several threat actors were seen targeting bugs in MobileIron servers and attempting to orchestrate intrusions inside company networks. Threat actors ranging from DDoS botnets to Chinese state-sponsored hacking groups have been observed exploiting severe vulnerabilities in MobileIron's MDM. The RCE vulnerability CVE-2020-15505 has turned out to be one of the most dangerous security flaws. Considering it as a gateway bug, MDM servers are likely to remain under attack with DDoS malware and other malware for the foreseeable future	
Source	https://blog.orange.tw/2020/09/how-i-hacked-facebook-again-mobileiron-mdm-rce.html
Infected Areas	MobileIron MDM
Recommendation	• Organizations to perform security audits of their MobileIron MDM server and internal networks. • Update the patch available

5. Multiple Address bar spoofing vulnerabilities

Description	
Cybersecurity researchers on Tuesday disclosed details about an address bar spoofing vulnerability affecting multiple mobile browsers, such as Apple Safari and Opera Touch, leaving the door open for spear-phishing attacks and delivering malware. The issue stems from using malicious executable JavaScript code in an arbitrary website to force the browser to update the address bar while the page is still loading to another address of the attacker's choice. an attacker can set up a malicious website and lure the target into opening the link from a spoofed email or text message, thereby leading an unsuspecting recipient into downloading malware or risk getting their credentials stolen.	
Source	https://www.rafaybaloch.com/2020/10/multiple-address-bar-spoofing-vulnerabilities.html
Infected Technology	Safari, Opera Touch, UCWeb, Yandex Browser, Bolt Browser, RITS Browser
Recommendation	Update the latest available patch released

For any queries/recommendations:

Contact us: **whois@cryptogennepal.com**