November 17, 2020

INFOSEC WEEKLY

#MADE4SECURITY

- **Pixar OpenUSD multiple vulnerabilities affects some version of macOS**
- **Nvidia warns of GeForce NOW flaw**
- **Google patched two Chrome 0-day vulnerabilities**
- **NPM caught stealing sensitive browser and Discord files**
- **WordPress Site takeovers**
- **Fake Microsoft Teams update**
- **Ubuntu fixes bug that standard user could use to become root**
- **Colossal Intel Update Anchored by critical Privilege-Escalation Bugs**

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. Pixar OpenUSD multiple vulnerabilities affects some version of macOS

Description

Pixar OpenUSD, software used by digital animation, contains multiple vulnerabilities that can be used by threat actors to perform various actions. The vulnerabilities can be used to corrupt memories allowing attacker to perform additional malicious action on victim's device. An update for the vulnerabilities has been released. The vulnerabilities exist due to how it handles memory resulting in disclosure of sensitive information while some can be escalated to execute arbitrary code.

Source	https://blog.talosintelligence.com/2020/11/vuln-spotlight-pixar-open-usd-nov-2020.html
Infected Technology	Pixar OpenUSD 20.05 and macOS Catalina 10.15.3 Pixar OpenUSD 20.08 and macOS Catalina 10.15.6
CVE_ID	CVE-2020-6155, CVE-2020-13494, CVE-2020-13495, CVE-2020-13496, CVE-2020-13498, CVE-2020-13520, CVE-2020-13524, CVE-2020-13531
Recommendation	Apply the update released

2. Nvidia warns of GeForce NOW flaw

Description

Nvidia has warned Windows gamers about a high-severity flaw in its GeForce NOW application software for Windows. The flaw can be exploited by network attacker to execute code or gain escalated privilege on affected device. OpenSSL library is vulnerable to binary planting attacks. The attacker can plant binary file that contains malicious code which is loaded and executed inside vulnerable application. Nvidia has also released details of other two flaw in its experience software affecting Windows version.

Source	https://nvidia.custhelp.com/app/answers/detail/a_id/5096
Infected Technology	GeForce NOW application for Windows before 2.0.25.119
CVE	CVE-2020-5992
Recommendation	Update the affected version

3. Google patched two Chrome 0-day vulnerabilities

Description

Google has released a new version of Chrome which has patched two more 0-days vulnerabilities that were exploited in the wild. The 0-day were due to improper implementation in V8, Chrome's JavaScript engine, and memory corruption in Site Isolation, Chrome's component used for sandboxing a site from another. Google has not disclosed the scenarios where the flaws were exploited and how many users are targeted but advises all user to update to the latest version.

Source	https://chromereleases.googleblog.com/2020/11/stable-channel-update-for-desktop_11.html
Infected Technology	Google Chrome
CVE	CVE-2020-16013, CVE-2020-16017
Recommendation	Update to Chrome 86.0.4240.198

4. NPM caught stealing sensitive browser and Discord files

Description

On November 9th, security researchers at Sonatype discovered a npm package named discord.dll containing malicious code designed to steal sensitive files from the victim's browser and Discord application. NPM is a JavaScript programming language packet manager. NPMs are used to load and update libraries for JavaScript projects by developers. According to the afore mentioned researchers, discord.dll, after installation runs the malicious code to search the victim's PC for certain applications and retrieve their internal levelDB Databases.

Source	https://blog.sonatype.com/discord.dll-successor-to-npm-fallguys-
Infected Areas	Google Chrome, Brave, Opera, Yandex, Discord

5. WordPress Site takeovers

Description

Wordfence, a Threat Intelligence team disclosed three security flaws that could allow the attackers to escalate their privileges to admin and take over any WordPress site that is using the Ultimate Member extensible WordPress plugin. Out of the three bugs, two received a maximum CVSS rating as they allowed unauthenticated privilege escalation via user meta and user roles and the third stood at 9.8/10 which allowed any authenticated attacker to elevate privileges to admin after wp-admin access to the site's profile .php page.

Source	https://www.wordfence.com/blog/2020/11/critical-privilege-escalation-vulnerabilities-affect-100k-sites-using-ultimate-member-plugin/
Infected Technology	Wordpress
Recommendation	Update the Ultimate Member plugin to 2.1.12

6. Fake Microsoft Teams update

Description

Fake Ads for the Microsoft Teams update have been going around to infect the systems with backdoors deploying Cobalt Strike. Used by ransomware operators, the attacks targeted education sector. Microsoft discovered that the perpetrators had purchased a search engine ad causing the top results for the Microsoft Teams software directing to their domain. The link downloaded a payload which in turn executed a PowerShell script to retrieve additional malicious content along with a legitimate copy of the Teams app to misdirect the victims.

Source	https://www.bleepingcomputer.com/news/security/fake-microsoft-teams-updates-lead-to-cobalt-strike-deployment/
Infected Technology	Microsoft Teams
Recommendation	Do not click on untrusted links Do not download software from unknown sources

7. Ubuntu Fixes bugs that standard users could use to become root

Description

Ubuntu developer have fixed a series of vulnerabilities that made it easy for standard user coveted root privileges. The first series of commands triggered a denial-of-service bug in a daemon called accounts service, which as its name suggests is used to manage user accounts on the computer. To do this, Backhouse created a Symlink that linked a file named .pam_environment to /dev/zero, changed the regional language setting, and sent accounts service a SIGSTOP. With the help of a few extra commands, Backhouse was able to set a timer that gave him just enough time to log out of the account before accounts service crashed. When done , Ubuntu would restart and open a window that allowed the user to create a new account that—you guessed it—had root privileges.

Source	https://securitylab.github.com/research/Ubuntu-gdm3-accountsservice-LPE
Infected Technology	Ubuntu 20.04
Recommendation	Update the latest patch available.

8. Colossal Intel Update anchored by critical Privilege-Escalation Bugs

Description

Intel introduced 40 security advisories in overall, addressing critical- and large-severity flaws across its Active Management Technology, Wireless Bluetooth and NUC products. A huge Intel security update this thirty day period addresses flaws across a myriad of items – most notably, critical bugs that can be exploited by unauthenticated cybercriminals in get to acquire escalated privileges. These critical flaws exist in items related to Wi-fi Bluetooth – which include many Intel Wi-Fi modules and wi-fi network adapters – as effectively as in its remote out-of-band administration device, Lively Administration Technology (AMT).

Source	https://threatpost.com/intel-update-critical-privilege-escalation-bugs/161087/?web_view=true
Infected Technology	Intel Products
Recommendation	Update the latest available patch by Intel

For any queries/recommendations:

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