December 7, 2020

INFOSEC WEEKLY

#MADE4SECURITY

- Android application using unpatched version of Play Core Libraries
- Eight security flaws identified in Google Chrome
- Multiple Botnets are Exploiting Critical Oracle WebLogic
- UEFI/BIOS Firmware are in affect with the TrickBot malware
- VMware fixes zero-day vulnerabilities reported by NSA
- About 8% of all Google Play apps are vulnerable to old security bug
- Zero-Click ‘Wormable’ vulnerability used to exploit iPhones
- Xerox DocuShare bugs allow data leaks

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. Android application using unpatched version of Play Core Libraries

Description

According to a research by Check Point, 8 out of 13 percentage of application in Play Store, using Android's Play Core Library, have not updated to patched version Play Core Library is used by applications to trigger in-ap updates and download additional language packs. This flaw can be used to form a path traversal vulnerability in the library that can be used to load and execute the malicious code on a target app to steal a user's sensitive data like user's login credentials, passwords, etc.

Source	https://research.checkpoint.com/2020/vulnerability-in-google-play-core-library-remains-unpatched-in-google-play-applications/
Infected Technology	Google Play Core Library prior 1.7.2
CVE	CVE-2020-8913
Recommendation	Developers: Update the play core libraries.

2. Eight security flaws identified in Google Chrome

Description

Google has now updated a total of 8 bugs from which four were high severity bugs. Three of the high severity vulnerabilities impacted the memory of Chrome's clipboard, media and extensions while the fourth impacts V8 JavaScript engine. The fourth vulnerability leads to cross-site scripting due to insufficient data validation. Google has rolled out an update for Windows, Mac and Linux to address the vulnerabilities.

Source	https://chromereleases.googleblog.com/2020/12/stable-channel-update-for-desktop.html
Infected Technology	Google Chrome
CVE	CVE-2020-16037, CVE-2020-16038, CVE-2020-16039, CVE-2020-16040, CVE-2020-16041, CVE-2020-16042
Recommendation	Update the chrome web browser to the latest version

3. Multiple Botnets are Exploiting Critical Oracle WebLogic

Description

Oracle WebLogic is a platform for developing, deploying, and running enterprise Java application. Multiple botnets are targeting thousands of publicly exposed and still unpatched Oracle WebLogic servers to deploy crypto miners and still sensitive information from information systems. According to Juniper Threat Labs, operators of the DarkIRC botnet are exploiting this vulnerability to spread laterally across the network, download files, records keystrokes, steal credentials, and execute arbitrary commands on compromised machines.

Source	https://thehackernews.com/2020/12/multiple-botnets-exploiting-critical.html
Infected Technology	Oracle WebLogic
CVE	CVE-2020-14882, CVE-2020-14750
Recommendation	Apply for the October 2020 Critical Patch Update

4. UEFI/BIOS Firmware are in affect with the TrickBot malware

Description

TrickBot, one of the most notorious and adaptable malware botnets in the world, is expanding its toolset to set its sights on firmware vulnerabilities to potentially deploy bootkits and take complete control of an infected system. With access to UEFI firmware, the malware can establish persistence in the compromised system that resists operating system reinstalls or replacing of storage drives. With UEFI, TrickBot operators can disable any OS level security controls they want, which then allows them to re-surface to a modified OS with neutered endpoint protections and carry out objectives with unhurried time on their side.

Source	https://eclypsium.com/2020/12/03/trickbot-now-offers-trickboot-persist-brick-profit/
Infected Technology	UEFI/BIOS firmware
Recommendation	Keep firmware up to date. Enable BIOS write protection. Verify firmware integrity to check against unauthorized modifications.

5. VMware fixes zero-day vulnerabilities reported by NSA

Description

VMware has released security updates related to the zero-day command injection vulnerabilities reported by the NSA. The command injection bug was in services such as: VMware Workspace One Access, Access Connector, Identity Manager and Identity Manager Connector. The bug was tracked as CVE-2020-4006. VMware has provided a workaround for admins to rectify the bug. Successful exploitation would let the attackers to escalate privileges and execute OS command on Linux and Windows Operating system.

Source	https://kb.vmware.com/s/article/81754
Infected Technology	VMware Workspace One Access 20.01, 20.10 (Linux) VMware Identity Manager (vIDM) 3.3.1 up to 3.3.3 (Linux) VMware Identity Manager Connector (vIDM Connector): Linux: 3.3.1, 3.3.2 Windows: 3.3.1, 3.3.2, 3.3.3 / 19.03.0.0, 19.03.0.1
CVE	CVE-2020-4006
Recommendation	Apply the patch released by the OEM

6. About 8% of all Google Play apps are vulnerable to old security bug

Description

Around 8% of all Android apps present on the Google Play Store are vulnerable to a security flaw popular in Android Library. This information is claimed from a scan carried out this fall by Check Point. The security flaw is present in the older versions of a java-based library called “Play Core” which lets the apps interact with the official Play Store Portal. Play Core is very popular as developers use it to download and install updates hosted on the Play Store. This flaw could lead to stealing sensitive information such as passwords, photos, 2 factor authentication codes and conducting easy data pilfering attacks.

Source	8% of all Google Play apps vulnerable to old security bug | ZDNet
Infected Technology	Microsoft Edge, Grindr, OKCupid, Cisco Teams, Viber and Booking.com
CVE	CVE-2020-8913
Recommendation	The applications should be updated to the latest version for security patch update.

7. Zero-Click 'Wormable' vulnerability used to exploit iPhones

Description

Google Project Zero researcher have disclosed a critical wormable vulnerability in Apple devices that allows attackers connected to the same network to gain complete control. Once exploited, attacker can view all photos, email, copy private messages and monitor device in real time. Apple has addressed the issue via security updates. The impact is due to a buffer overflow error in Wi-Fi driver associated with Apple Wireless Direct Link (AWDL), protocol used in AirDrop and AirPlay that enables easier communication between Apple devices.

Source	https://googleprojectzero.blogspot.com/2020/12/an-ios-zero-click-radio-proximity.html
Infected Technology	MacOS, iOS and watchOS
CVE	CVE-2020-3843
Recommendation	Update the security updates for OS 13.3.1, macOS Catalina 10.15.3, and watchOS 5.3.7

8. Xerox DocuShare bugs allow data leaks

Description

Xerox has released security updates for DocuShare to address a vulnerability that could allow an unauthenticated attacker to obtain sensitive information. The vulnerabilities open Solaris, Linux and Windows Docushare users up to both a server-side request forgery attack and an unauthenticated external XML entity attack. A SSRF vulnerability would allow an attacker to abuse functionality on a server hosting the software-as-a-service (SaaS) DocuShare. A successful SSRF attack typically allows an adversary to read or update internal resources. An XXE is a type of attack against an application that parses XML input. This attack occurs when XML input containing a reference to an external entity is processed by a weakly configured XML parser.

Source	https://securitydocs.business.xerox.com/wp-content/uploads/2020/11/cert_Security_Mini_Bulletin_XRX20W_for-DocuShare-6.61_7.0_7.5.pdf
Infected Technology	Docushare version 6.6.1, 7.0 , 7.5
CVE	CVE-2020-27177
Recommendation	Update the latest Security updates released By Xerox

For any queries/recommendations:

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