INVINSENSE™
Attacktical Cybersecurity Sense

Infopercept

INFOPERCEPT NEWSLETTER

ISSUE -20 September 2021

Contents

"IT TAKES 20 YEARS TO BUILD A REPUTATION AND FEW MINUTES OF CYBER-INCIDENT TO RUIN IT."

– STEPHANE NAPPO

Patches Notes

MICROSOFT FIXES REMAINING WINDOWS PRINTNIGHTMARE VULNERABILITIES

- Microsoft has issued a security update to address the last remaining PrintNightmare zero-day vulnerabilities, which allowed attackers to quickly obtain administrative access to Windows systems.
- Despite the fact that Microsoft provided two security fixes to address multiple PrintNightmare vulnerabilities, another publicly revealed vulnerability still allowed threat actors to get SYSTEM rights by connecting to a remote print server.

MICROSOFT SEPTEMBER 2021 PATCH TUESDAY

- The most critical of the freshly issued security notes corrects a problem with SAP NetWeaver Application Server for Java's authorisation check. The vulnerability has a CVSS score of 10 and is identified as CVE-2021-37535.
- An erroneous input sanitization in 25 RFC-enabled function modules might allow a "authenticated user with certain particular rights to remotely call these function modules and run modified queries to get access to the backend database," according to the problem.

THIRD CRITICAL BUG AFFECTS NETGEAR SMART SWITCHES

- Critical vulnerability in Netgear smart switches that could be leveraged by an attacker to potentially execute malicious code and take control of vulnerable devices.
- This could grant a hacker the ability to change the administrator password without actually having to know the previous password or hijack the session.

CYBER ATTACKS

CREDENTIAL LEAK FEARS RAISED FOLLOWING SECURITY BREACH AT TRAVIS CI

- A forked public repository might submit a pull request (common feature in GitHub, BitBucket, and Assembla) and gain unlawful access to secret from the original public repository in exchange for printing some of the flies throughout the build process.
- All public repositories were injected into PR [pull request] builds, and secrets were encrypted in the Travis CI database in this situation.

WALGREENS' COVID-19 TEST REGISTRATION SYSTEM EXPOSED PATIENT DATA

- Personal information such as your name, date of birth, gender identification, phone number, address, and email address was left on the open web for anyone to access and for ad trackers on Walgreens' website to capture. Even the outcomes of these tests could be obtained from that data in some situations.
- The issues are with Walgreens' Covid-19 test appointment registration system, which everyone who wants a Walgreens test must use (unless they purchase an over-the-counter test)

FREE REVIL RANSOMWARE MASTER DECRYPTER RELEASED FOR PAST VICTIM

- A free master decryptor for the REvil ransomware operation has been released, allowing all victims encrypted before the gang disappeared to recover their files for free.
- REvil ransomware victims can download the master decryptor from Bitdefender (instructions) and decrypt entire computers at once or specify specific folders to decrypt.

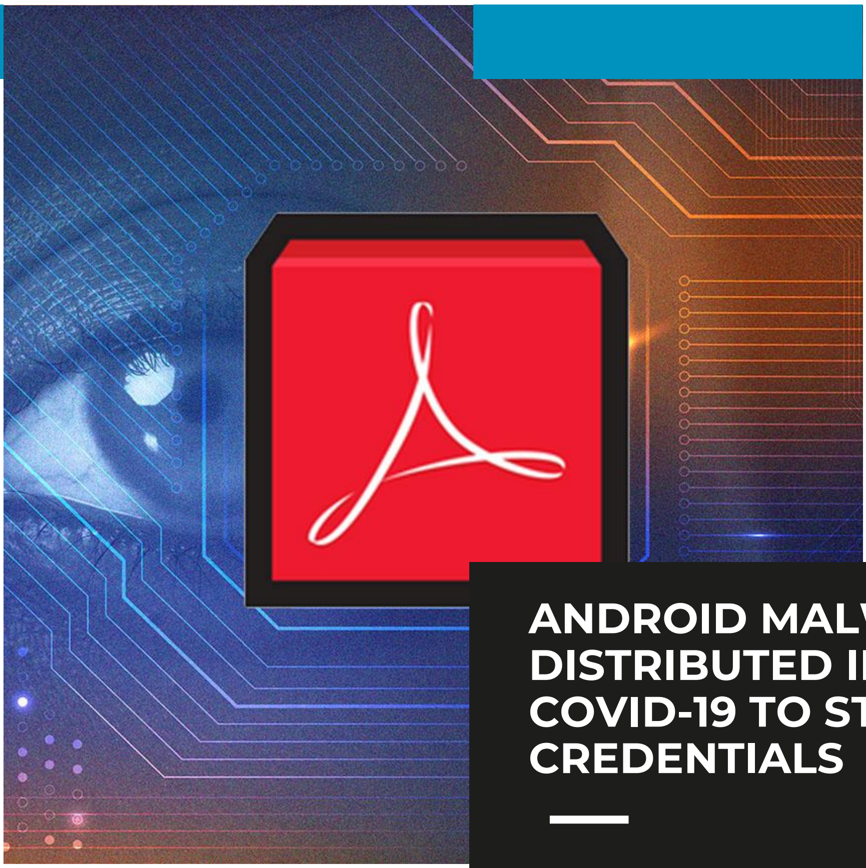
OVER 60 MILLION WEARABLE, FITNESS TRACKING RECORDS EXPOSED VIA UNSECURED DATABASE

- GetHealth, based in New York, bills itself as a one-stop shop for health and wellness data from hundreds of wearables, medical devices, and apps.
- The data warehouse held over 61 million records, including enormous swaths of user data, some of which may be considered sensitive, such as names, dates of birth, weight, height, gender,

Malware and Vulnerabilities

REMOTE CODE EXECUTION FLAW ALLOWED HIJACK OF MOTOROLA HALO+ BABY MONITORS

- Baby monitors may have been hijacked if remote code execution (RCE) and communications protocol flaws had been detected and fixed.
- Hubble Connected pulls information beyond simply the monitor's camera feed and presents it in the user's display. This data includes room temperature, night lights, and the status of the monitor's light show projector



ANDROID MALWARE DISTRIBUTED IN MEXICO USES COVID-19 TO STEAL FINANCIAL CREDENTIALS

- This malware can take authentication elements that are required to access accounts at the targeted financial institutions in Mexico from their victims.
- A malicious phishing page spreads the infection by offering real financial security suggestions (copied from the genuine bank site) and recommending downloading the malicious apps as a security tool or an app to report out-of-service. ATM

CODE EXECUTION VULNERABILITY IN NITRO PRO PDF

- A vulnerability in the Nitro Pro PDF reader was recently found by Cisco Talos, which might allow an attacker to execute malware in the context of the programme.
- It supports numerous capabilities for parsing PDFs via third-party libraries. The TALOS-2021-1267 (CVE-2021-21798) vulnerability is a use-after-free flaw that can be exploited if a target opens a specially designed malicious PDF.

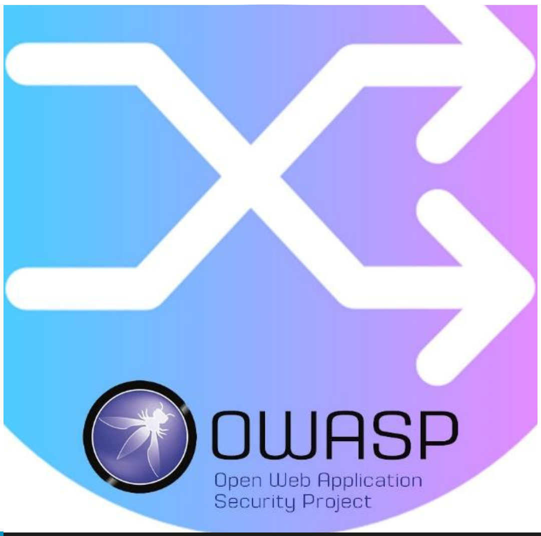
ADOBE SNUFFS CRITICAL BUGS IN ACROBAT, EXPERIENCE MANAGER

- Adobe is advising Acrobat Reader customers to upgrade their software to fix significant flaws that might allow attackers to run arbitrary code on unpatched versions.
- In total, 36 of the issues are labelled "critical," which is an Adobe-specific classification that indicates that if exploited, the defects might allow malicious native-code to execute without the user's knowledge.

CYBER TECH

MICROSOFT ROLLS OUT PASSWORDLESS LOGIN FOR ALL MICROSOFT ACCOUNTS

- Microsoft will begin rolling out passwordless login functionality in the coming weeks, allowing customers to access their Microsoft accounts without having to provide a password.
- This feature will help secure your Microsoft account from phishing attacks while also making access to the top apps and services like Microsoft 365, Microsoft Teams, Outlook, OneDrive, Family Safety, Microsoft Edge, and others even easier.



OWASP RESHUFFLES ITS TOP 10 LIST, ADDS NEW CATEGORIES

- The Open Web Application Security Project reshuffles its list of top threats as well including three new risk categories.
- Cross-Site Scripting (XSS), which accounts for about one in every five disclosed vulnerabilities, disappeared from the list,

FACEBOOK AND DROPBOX NEW PARTNERSHIP

- Dropbox has partnered with Facebook on a digital transfer project which will allow users to import data directly from their social media accounts.
- The files will transfer to Dropbox in the background the user will have control over who exactly has access to the photos and videos.

ABOUT INFOPERCEPT

Infopercept's vision and core values revolve around making organizations more secure through the core values of Honesty, Transparency and Knowledge, so as to enable them to make better informed decisions about their security practices & goals. With our synergistic vision to combine technical expertise and professional experience, we aim to further establish our place as a one stop shop for our clients and partners' cybersecurity and accreditation needs.

Our specialized core team comprises experienced veterans, technical experts & security enthusiasts having good practical experience & thorough knowledge in the Cybersecurity domain, latest trends, and security innovations; ensuring that you always get the best security approach & solution for your specific business needs exactly the way you want it to be.

MANAGED SECURITY SERVICES

Cybersecurity Monitoring and Management Services

There is a global need for expertise in managing complex IT Security Infrastructures. Infopercept provides IT Security and Infrastructure services as a Managed Security Service Provider (MSSP) and is a leading contributor in this segment. Infopercept delivers Managed Security Services globally in line with industry leading security policies, frameworks and technologies. We are powered by an inhouse team of highly competent cybersecurity professionals with vast practical exposure. Our practices have been developed over the years to protect client interests and fulfill their needs.

Infopercept
SECURE • OPTIMIZE • STRENGTHEN

+91 98988 57117
sos@infopercept.com
www.infopercept.com

INVINSENSE™
Attacktical Cybersecurity Sense