February 22, 2021

INFOSEC WEEKLY

#MADE4SECURITY

- Apple patches severe macOS Big Sur data loss bug
- Hackers can bypass Mastercard PIN, using them as visa card
- Security bugs left unpatched in Android app with one billion downloads
- Command injection vulnerability found in vSphere Replication
- OpenSSL patches three new vulnerabilities
- SQLite patches use-after-free bugs leading to code execution and denial-of-service exploits
- Ninja Forms WordPress Plugin Bug Opens Websites to Hacks
- Malvertisers Exploited WebKit 0-Day to Redirect Browser Users to Scam Sites

CryptoGen Nepal

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. Apple patches severe macOS Big Sur data loss bug

Description
For the past few weeks, macOS Big Sur has suffered from a bug that could cause serious data loss. The bug was primarily introduced in Big Sur 11.2 which then later made its way to the 11.3 data. The bug comes down to the macOS Big Sur installer not checking if the Mac has the required free space available to carry out an upgrade. The upgrade runs into problems, and if that isn't bad enough, if the user's Mac was encrypted using FileVault, then the user is locked out of their data. Thankfully, Apple has now finally released an updated macOS Big Sur 11.2.1 installer that properly checks for free space.

Source	https://mrmacintosh.com/big-sur-upgrade-not-enough-hd-space-serious-issue-possible-data-loss/
Infected Technology	Big Sur 11.2, Big Sur 11.3
Recommendation	• Consider installing the updated release of macOS Big Sur 11.2.1 installer (20D75) • Consider checking the system requirements without completely relying on the installer to check everything.

2. Hackers can bypass Mastercard PIN, using them as visa card

Description
Cybersecurity researchers have disclosed a novel attack that could allow criminals to trick a point-of-sale terminal into transacting with a victim's Mastercard contactless card while believing it to be a Visa card. The research, published by a group of academics from ETH Zurich, builds on a study detailed last September that delved into a PIN bypass attack, permitting bad actors to leverage a victim's stolen or lost Visa EMV-enabled credit card for making high-value purchases without knowledge of the card's PIN, and even fool the terminal into accepting unauthentic offline card transactions.

Source	https://emvrace.github.io/
Infected Technology	Visa card and MasterCard
Recommendation	• Consider keeping your visa card in a secured manner. • If lost, contact the concerned parties for blocking your visa card.

3. Security bugs left unpatched in Android app with one billion downloads

Description	
An android application downloaded more than one billion times contains unpatched vulnerabilities that the app maker has failed to fix for more than three months. The vulnerabilities impact the Android version of SHAREit, a mobile app that allows users to share files with friends or between personal devices. The bugs can be exploited to run malicious code on smartphones where the SHAREit app is installed, after which the legitimate features can be used to run custom code, overwrite the apps' local files, or installation of third-party apps could be done without the user's knowledge. The root cause of these security flaws is the lack of proper restrictions on who can tap into the applications' code.	
Source	https://www.trendmicro.com/en_us/research/21/b/shareit-flaw-could-lead-to-remote-code-execution.html?ClickID=cpnlq7vpz7fzvpwqxeivvs7lqwnwepkkkkz
Infected Technology	Android phones with SHAREit app installed.
Recommendation	Consider updating the SHAREit app to its latest version.

4. Command injection vulnerability found in vSphere Replication

Description	
vSphere Replication 8.3.x prior to 8.3.1.2, 8.2.x prior to 8.2.1.1, 8.1.x prior to 8.1.2.3, and 6.5.x prior to 6.5.1.5 contain a post-authentication command injection vulnerability in the "Startup Configuration" page which may allow an authenticated admin user to perform remote code execution. VMware has evaluated this issue to be 'Important' severity with a maximum CVSSv3 base score of 7.2. Egor Dimitrenko, the Positive Technologies researcher who discovered the vulnerability said, "An attacker could obtain the access required for exploitation through, for example, social engineering or by hoping that the targeted admin account is protected by a weak password".	
Source	https://www.vmware.com/security/advisories/VMSA-2021-0001.html
Infected Technology	vSphere Replication
CVE-ID	CVE-2021-21976
Recommendation	Consider applying security patches released by VMware.

5. OpenSSL patches three new vulnerabilities

Description	
OpenSSL Project has released patches of three vulnerabilities leading to two denial-of-service (DoS) attacks and incorrect SSLv3 rollback protection. The flaws were identified by Google Project Zero researcher Travis Ormandy. The DoS-based vulnerability was caused as a result of a NULL pointer dereference issue that results in a crash. Another security hole is related to an X509_issuer_and_serial (hash impact the application that uses the function directly with the certificates obtained from untrusted sources.	
Source	https://www.openssl.org/news/secadv/20210216.txt
Infected Technology	OpenSSL 1.0.2 and 1.1.1
CVE-ID	CVE-2021-23841, CVE-2021-23840, CVE-2021-23439
Recommendation	Consider updating OpenSSL to its latest version.

6. SQLite patches use-after-free bugs leading to code execution and denial-of-service exploits

Description	
SQLite has Patched a use-after-free bug that could lead to arbitrary code execution or denial of service (DoS) if triggered. SQLite is built into over 3.5 billion active smartphones and includes Apple Macs, Windows 10 machines, web browsers, iTunes, Skype, and other applications. The issue had arisen in SQLite's SELECT query functionality. There was a problem handling sub-queries due to the code change implementation performed during June of 2020. The exploitation of the vulnerability depends on the attacker having access to the query the data in the database hence, is marked as medium severity.	
Source	https://bugzilla.redhat.com/show_bug.cgi?id=1924886
Infected Technology	SQLite 3 release line
CVE-ID	CVE-2021-20227
Recommendation	Consider updating SQLite to its latest version.

7. Ninja Forms WordPress Plugin Bug Opens Websites to Hacks

Description	
Ninja Forms, a WordPress plugin used by over a million sites is vulnerable allowing remote attackers to create numerous problems and WordPress site takeover. The four bugs found lets users with low privileges carry out malicious activities that include eavesdropping on on-site email, installing arbitrary add-ons, redirecting site owners to malicious destinations, and takeover over the admin account. The email hijacking capability could also be capitalized by the hackers to route the mail from the WordPress site for authenticating the attackers in the SendWP account. This would eventually lead to remote code execution and site takeover as the admin account was compromised.	
Source	https://www.wordfence.com/blog/2021/02/one-million-sites-affected-four-severe-vulnerabilities-patched-in-ninja-forms/
Infected Technology	Ninja Forms versions <= 3.4.33
Recommendation	Consider installing the patched version (3.4.34) of Ninja Forms.

8. Malvertisers Exploited WebKit 0-Day to Redirect Browser Users to Scam Sites

Description	
A malvertising group known as "ScamClub" exploited a zero-day vulnerability in WebKit-based browsers to inject malicious payloads that redirected users to fraudulent websites gift card scams. The attack leveraged a bug that allowed malicious parties to bypass the iframe sandboxing policy in the browser engine that powers Safari and Google Chrome for iOS and run malicious code. Specifically, the technique exploited the manner how WebKit handles JavaScript event listeners, thus making it possible to break out of the sandbox associated with an ad's inline frame element despite the presence of the "allow-top-navigation-by-user-activation" attribute that explicitly forbids any redirection unless the click event occurs inside the iframe.	
Source	https://blog.confiant.com/malvertiser-scamclub-bypasses-iframe-sandboxing-with-postmessage-shenanigans-cve-2021-1801-1c998378bfba
Infected Technology	WebKit-based browsers
CVE-ID	CVE-2021-1801
Recommendation	Consider ignoring suspicious giftcards while browsing internet.

9. Privacy Bug in Brave Browser Exposes Dark-Web Browsing History of Its Users

Description	
Brave has fixed a privacy issue in its browser that sent queries for .onion domains to public internet DNS resolvers rather than routing them through Tor nodes, thus exposing users' visits to dark web websites. This is achieved by relaying users' requests for an onion URL through a network of volunteer-run Tor nodes. At the same time, it's worth noting that the feature uses Tor just as a proxy and does not implement most of the privacy protections offered by Tor Browser. But according to a report first disclosed on Ramble, the privacy-defeating bug in the Tor mode of the browser made it possible to leak all the .onion addresses visited by a user to public DNS resolvers.	
Source	https://brave.com/latest/
Infected Technology	Brave Browser
Recommendation	Consider Updating Brave browser

10. Cred-stealing trojan harvests logins from Chromium browsers, Outlook, and more, warns Cisco Talos

Description	
A credential-stealing trojan that lifts your login details from the Chrome browser, Microsoft's Outlook and instant messengers have been uncovered by Cisco Talos. Delivered through phishing emails, the Masslogger trojan's latest variant is contained within a multi-volume RAR archive using the .chm file format and .roo extensions, said Switchzilla's security research arm. Apps vulnerable to these dastardly cred-stealing doings include Discord, Microsoft Outlook, Mozilla Thunderbird, Firefox, and Chromium-based browsers. The malware also tries to exclude itself from Windows Defender scans.	
Source	https://blog.talosintelligence.com/2021/02/masslogger-cred-exfil.html
Infected Technology	Microsoft outlook, Chromium Browsers, and Instant Messengers
Recommendation	Consider not opening suspicious emails.

For any queries/recommendations:

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