Infopercept

INVINSENSE™
Attacktical Cybersecurity Sense

INFOPERCEPT NEWSLETTER

ISSUE -19 July 2021

Contents

QUANTUM ENCRYPTION IS ESSENTIAL TO PROTECT OUR DIGITAL ASSETS AND INFRASTRUCTURE FROM ATTACKERS.

Patches Notes

UPDATE WINDOWS PCS PATCH NEW FLAWS, INCLUDING 9 ZERO-DAYS

- The list of Patch Tuesday updates for July 2021 appears to be infinite.There are 117 patches with at least 42 CVEs attributed to them, with FAQs, mitigation information, or workarounds published for each.
- According to Microsoft, six vulnerabilities have already been published, and four are now being exploited in the wild. Aside from the ongoing PrintNightmare, yes, nightmare, there are a few others that need your full attention.

ADOBE UPDATES FIX 28 VULNERABILITIES IN 6 PROGRAMS

- Adobe has issued a massive Patch Tuesday security update that addresses vulnerabilities in Adobe Dimension, Illustrator, Framemaker, Acrobat, Reader, and Bridge.
- Adobe patched 28 vulnerabilities in all. As observed all the critical flaws may lead to arbitrary code execution, allowing threat actors to execute commands on affected systems.

KASEYA RELEASES PATCHES FOR FLAWS EXPLOITED IN WIDESPREAD RANSOMWARE ATTACK

- Kaseya released urgent upgrades on Sunday to fix significant security flaws in its Virtual System Administrator (VSA) product, which was used to target up to 1,500 organisations worldwide as part of a massive supply-chain ransomware assault.
- Following the incident, the business advised on-premises VSA clients to disable their servers until a fix was ready. Almost ten days later, the company has released VSA version 9.5.7a (9.5.7.2994), which includes solutions for three additional security vulnerabilities.

CYBER ATTACKS

MICROSOFT OFFICE USERS WARNED ON NEW MALWARE-PROTECTION BYPASS

- Microsoft Excel legacy users are being targeted in a malware campaign that use a unique malware-obfuscation method to deactivate Office protections and deliver the Zloader trojan.
- Zloader is a banking trojan that is designed to steal login passwords and other sensitive information from users of certain financial institutions. The malicious assault combines features in Microsoft Office Word and Excel to work together to download the Zloader payload without raising an alert message for end users.

"GUESS" FASHION RETAILER DATA BREACH AFTER RANSOMWARE ATTACK

- Guess, an American fashion brand and retailer, is alerting impacted consumers of a data breach that occurred as a result of a February ransomware assault that resulted in data theft.
- On June 3, 2021, the fashion shop determined the addresses of all impacted individuals after conducting a thorough assessment of the documents kept on compromised systems. On June 9, Guess began issuing breach notification letters to affected consumers, offering free identity theft protection services and a year of free credit monitoring through Experian to all impacted people.

MORGAN STANLEY ATTACK BREACH OF CUSTOMER SSNS

- Morgan Stanley has reported that one of its suppliers was compromised by the Accellion FTA vulnerability, and that certain client information, including Social Security numbers, was obtained.
- The vendor's files contained the following paricipant information: name; address (last knwn address); date of birth; and Social Security number (if the participant had one). as well as the corporate business name

Malware and Vulnerabilities

UPDATED JOKER MALWARE SURGE ANDROID APPS

- According to experts, the Joker mobile virus is back on Google Play, with an increase in malicious Android applications that disguise the billing-fraud software. It is also employing novel methods to avoid Google's app-vetting procedure.
- Since September, at least 1,000 additional samples have been identified in the newest wave, with many of them making their way into the legitimate market.

HTTP REQUEST SMUGGLING VULNERABILITY IN APACHE TOMCAT 'HAS BEEN PRESENT SINCE 2015'

- A HTTP request smuggling vulnerability in Apache Tomcat has been present "since at least 2015," according to the project maintainers.
- HTTP request smuggling is a hacking method that may be used to disrupt how a website handles sequences of HTTP requests sent by one or more users.

FLAW IN PREPROCESSOR LANGUAGE LESS.JS CAUSES WEBSITE TO LEAK AWS SECRET KEYS

- Researchers have cautioned that a vulnerability in the popular preprocessor language Less.js may be used to accomplish remote code execution (RCE) against websites that enable users to enter Less.js code.
- When the Less code is executed on the client side, it results in cross-site scripting (XSS), but when executed on the server side, it results in RCE.

WINDOWS HELLO BYPASS FOOLS BIOMETRICS SAFEGUARDS IN PCS

- A flaw in Microsoft's Windows 10 password-free authentication system has been discovered, which may allow an attacker to fake a picture of a person's face in order to fool the facial-recognition system and gain control of a computer.
- To exploit the Windows Hello bypass vulnerability, CVE-2021-34466, an attacker must have physical access to a device.

CYBER TECH

FIREFOX BECOMES LATEST BROWSER TO SUPPORT FETCH METADATA REQUEST HEADERS

- Mozilla has announced that Firefox now supports Fetch Metadata request headers, further safeguarding users from a variety of high-impact online assaults.

- Firefox 90 will have four new headers – Dest, Mode, Site, and User – that will allow web apps to protect users against numerous cross-origin threats such as cross-site request forgery (CSRF), cross-site leaks (XS-Leaks), and Spectre-style side-channel attacks.

WINDOWS 365 - MICROSOFT'S NEW VIRTUALIZED CLOUD PC SERVICE

- Microsoft has announced the much-anticipated cloud-based Windows 365 service, which is a virtualized desktop service that allows organisations to build and stream Cloud PCs from Azure.

- Windows 365 migrates the operating system to the Microsoft Cloud, securely streaming the whole Windows experience – including all of your programmes, data, and settings – to your personal or business devices. The Cloud PC is a whole new personal computer category created particularly for the hybrid world as a result of this strategy.

FACEBOOK ANNOUNCES TIME BONUS PAYOUTS FOR BUG HUNTERS

- Facebook is expanding its bug bounty programme to include a new perk that will pay researchers a bonus based on the time it takes the social network to remedy a vulnerability once it is discovered and reported by bug hunters

- According to Facebook, the Payout Time Bonus will reward reports that are paid more than 30 days after Facebook gets all of the required information for a successful replication of the report and its impact.

Infopercept

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.

TECHNICAL ASSESSMENT SERVICES

All organizations are just a single data breach away from being the lead story on the news and social media, which can severely damage an organization's brand reputation. Regular security assessments helps in identifying your most significant vulnerabilities. You can thus focus on targeting opportunities for improvement that offer the highest return on investment.

Infopercept's Technical Assessment Services provides key "inputs" of a security roadmap; where a thorough cyber security assessment evaluates your organizations's technology, policies, and awareness.

In order to understand the security needs of an organization, it is important to study in depth the organization's profile and its vulnerable areas. Infopercept's Security Assessment Services delivers the best possible service by using a combination of standardized methodologies along with it's own internal processes.

Infopercept
SECURE • OPTIMIZE • STRENGTHEN

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

INVINSENSE™
Attacktical Cybersecurity Sense