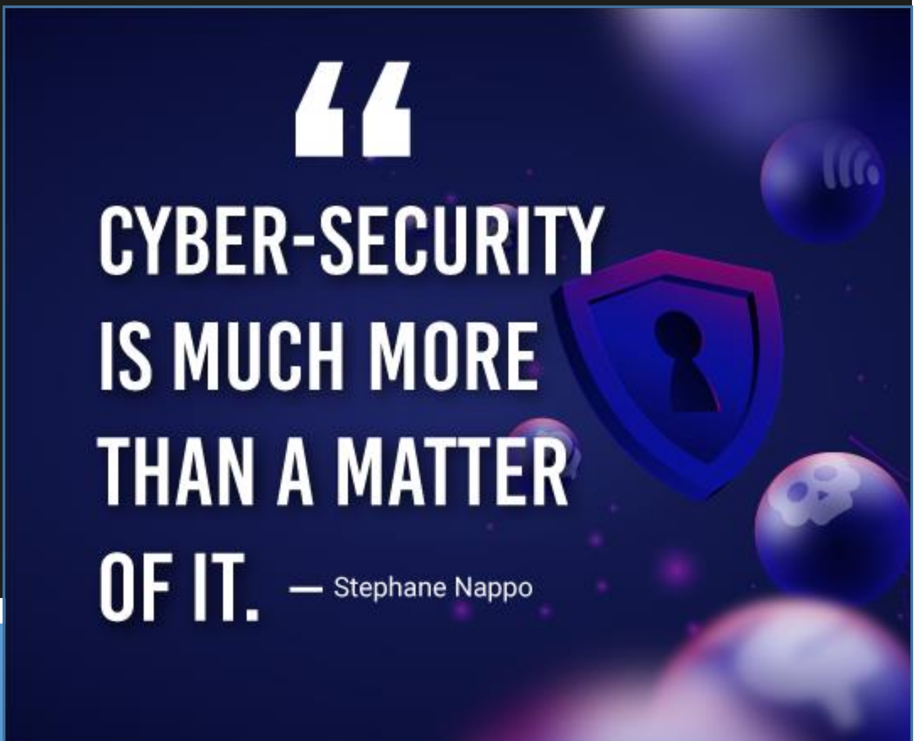
INVINSENSE™
Attacktical Cybersecurity Sense

Infopercept

INVINSENSE SECURITY AWARENESS BULLETIN

ISSUE - 4 October 2021

Contents



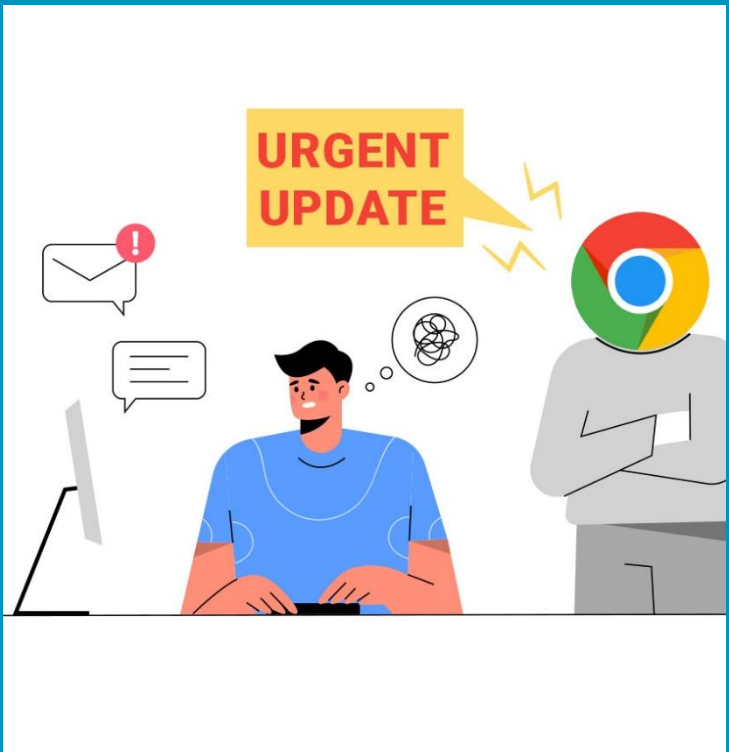
Patches Notes

TREND MICRO PATCHES CRITICAL VULNERABILITY IN SERVER PROTECTION SOLUTION

- Trend Micro has published remedies for Trend Micro Server Protect's major authentication bypass vulnerability.
- Virus, spyware, and rootkit protection for servers is provided by this enterprise-grade real-time malware detection solution, which also automates security operations.

MULTIPLE VULNERABILITIES IN MICROSOFT EDGE COULD ALLOW FOR ARBITRARY CODE EXECUTION

- Multiple vulnerabilities have been discovered in Microsoft Edge, the most severe of which could result in remote code execution.
- We recommend to Apply the security updates provided by Microsoft to vulnerable systems immediately and Run all software as a non-privileged user (one without administrative privileges).



CHROME UPDATE RELEASED TO PATCH ACTIVELY EXPLOITED ZERO-DAY VULNERABILITY

- Google rolled out an emergency security patch to its Chrome web browser to address a security flaw that's known to have an exploit in the wild.
- The vulnerability has been described as use after free in Portals API, a web page navigation system that enables a page to show another page as an inset and "perform a seamless transition to a new state, where the formerly-inset page becomes the top-level document."

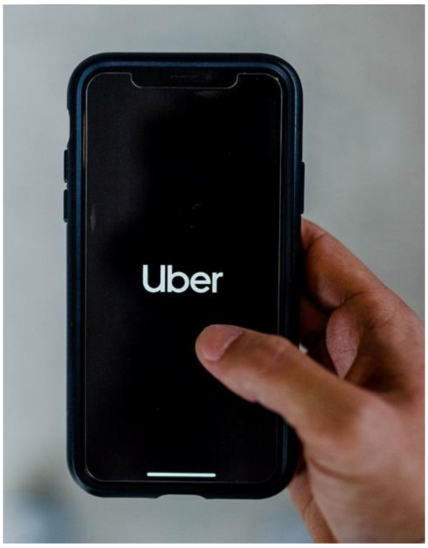
CYBER ATTACKS

NAVISTAR CONFIRMS DATA BREACH INVOLVED EMPLOYEE HEALTHCARE INFORMATION

- According to an updated Navistar statement on the breach, the potentially vulnerable data includes the full names, residences, dates of birth, and Social Security numbers of an undefined number of Navistar workers, both past and present.
- Cybercriminals frequently utilise and trade compromised personal data because it allows them to run more convincing phishing scams that seek even more information, or to apply for fraudulent lines of credit under fictitious names.

GRIFTHORSE ANDROID TROJAN STEALS MILLIONS FROM OVER 10 MILLION VICTIMS GLOBALLY

- GriftHorse malicious Android apps appear to be harmless, but this false sense of security is shattered when customers are paid month after month for the premium service they were subscribed to without their knowledge or agreement.
- The effort targeted millions of people in over 70 countries by sending targeted infected sites depending on their IP addresses geo-location and local language.



UBER SECURITY ALERT SCAM SPOOFS REAL UBER NUMBER—WATCH OUT!

- The alert received are pretty convincing and used the kind of language we're used to seeing in genuine security emails and SMS messages but fake security alert came from the phone number that the real Uber uses to send messages.
- The scammers first ask for Phone No, then they show that your account is locked after entering that.

COLOSSUS RANSOMWARE HITS AUTOMOTIVE COMPANY IN THE U.S.

- The Colossus ransomware, which targets Windows PCs, was used in an attack on a U.S.-based automobile group of dealerships, with its operators threatening to expose 200 GB of stolen data.
- While there isn't yet a public Colossus-specific ransomware leak site, one could appear in the coming weeks to leak data from a victim who refuses to pay the ransom.

Malware and Vulnerabilities

APPLE AIRTAG BUG ENABLES ‘GOOD SAMARITAN’ ATTACK

- If the Air Tag has been set to lost mode, the new Apple Air Tag tracking device has a function that lets anyone who discovers one of these tiny position beacons to scan it with a mobile phone and know its owner's phone number.

- Set it to Lost Mode, which generates a unique URL at https://found.apple.com and allows the user to leave a customised message and phone number.

Hackers Targeting Brazil's PIX Payment System to Drain Users' Bank Accounts

- Two recently discovered malicious Android applications have been used to target users of Brazil's immediate payment ecosystem in an apparent attempt to deceive victims into fraudulently transferring their whole account balances into a bank account under attackers' control.

- When a user launches their PIX bank app, Pixstealer displays an overlay window in which the victim cannot see

DOPPELDRIDEX DELIVERED VIA SLACK AND DISCORD

- A variant of the Dridex banking malware has been attempted to be delivered using payloads placed on Slack and Discord CDNs in several recent phishing attempts.

- Maldocs are attached to emails in these campaigns, which typically use an invoice-based or tax-themed social engineering bait. The sheet macro is run if the user selects contented.

TA544 TARGETS ITALIAN ORGANIZATIONS WITH URSNIF MALWARE

- TA544 is a cybercriminal threat actor that spreads banking malware and other payloads throughout the world, including Italy and Japan. And Ursnif is a Trojan that uses web injections, proxies, and VNC connections to steal information from websites.

- Once the Ursnif payload was deployed on the target machine, recent TA544 Ursnif campaigns included activity that targeted several sites using web injects and redirections.

CYBER TECH

NEW MICROSOFT EXCHANGE SERVICE MITIGATES HIGH-RISK BUGS AUTOMATICALLY

- Microsoft has released a new Exchange Server feature that applies interim mitigations for high-risk (and likely actively exploited) security weaknesses in order to protect on-premises systems from inbound attacks and allow administrators more time to implement security patches.

- It detects Exchange Servers that are vulnerable to one or more known threats and implements interim mitigations until a security update is available for administrators to apply.

GOOGLE LAUNCHES NEW REWARD PROGRAM FOR TSUNAMI SECURITY SCANNER

- The new Tsunami Security scanner is intended to scan large-scale company networks for open ports before cross-checking vulnerability exposure based on the first reconnaissance findings.

- Vulnerabilities such as Remote Code Executions (RCEs), unauthorised file uploading, security misconfigurations that expose sensitive admin panels, and so on are common examples.

MICROSOFT GETS WINDOWS 11 READY FOR RELEASE WITH NEW BUILDMAJIDI QUOTED

- Microsoft has moved Windows 11 to the Windows Insider 'Release' channel in anticipation of its upcoming launch on October 5th.

- Starting 23rd Sep, Microsoft is offering Windows 11 as an optional download within Windows Update for users with compatible hardware

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.

TECHNOLOGY ADVISORY SERVICES

One of the most critical components of a successful business is technology. But is your current technology in line with your organization's roadmap to success?

The right technology in your organization will help your business make the best use of the information and the resources, whilst empowering you to execute to the best of your abilities at functional and strategic levels. However, successful technology involves much more than just choosing a system. An organization should have the right balance of people, processes, and technology, so that it will help your business to grow.

Infopercept
SECURE • OPTIMIZE • STRENGTHEN

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

INVINSENSE™
Attacktical Cybersecurity Sense