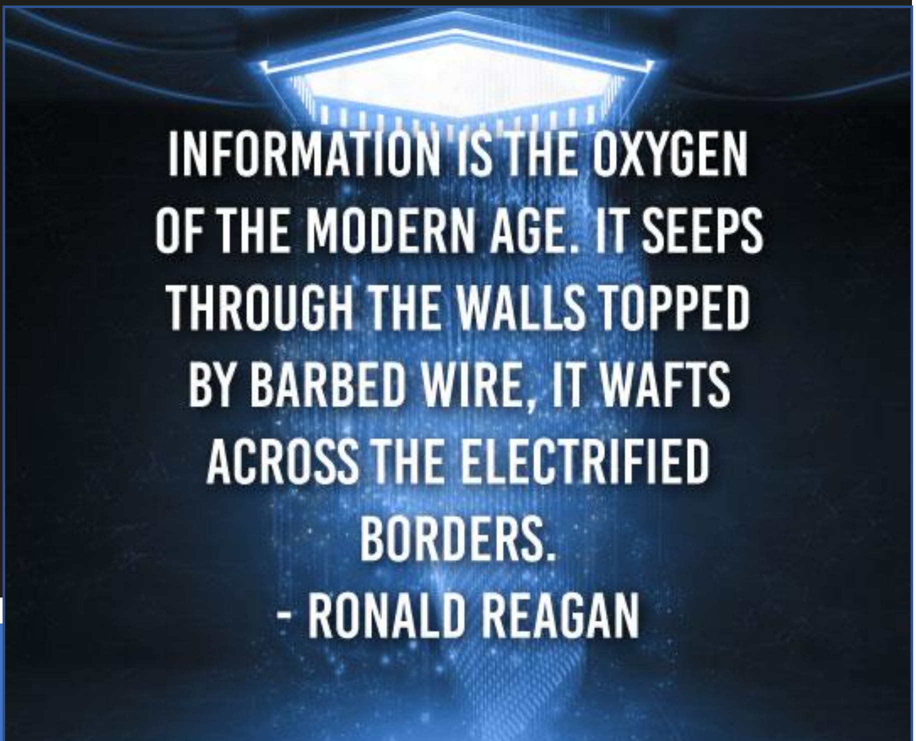
INVINSENSE™
Attacktical Cybersecurity Sense

Infopercept

INFOPERCEPT NEWSLETTER

ISSUE -23 Aug 2021

Contents



INFORMATION IS THE OXYGEN OF THE MODERN AGE. IT SEEPS THROUGH THE WALLS TOPPED BY BARBED WIRE, IT WAFTS ACROSS THE ELECTRIFIED BORDERS.
- RONALD REAGAN

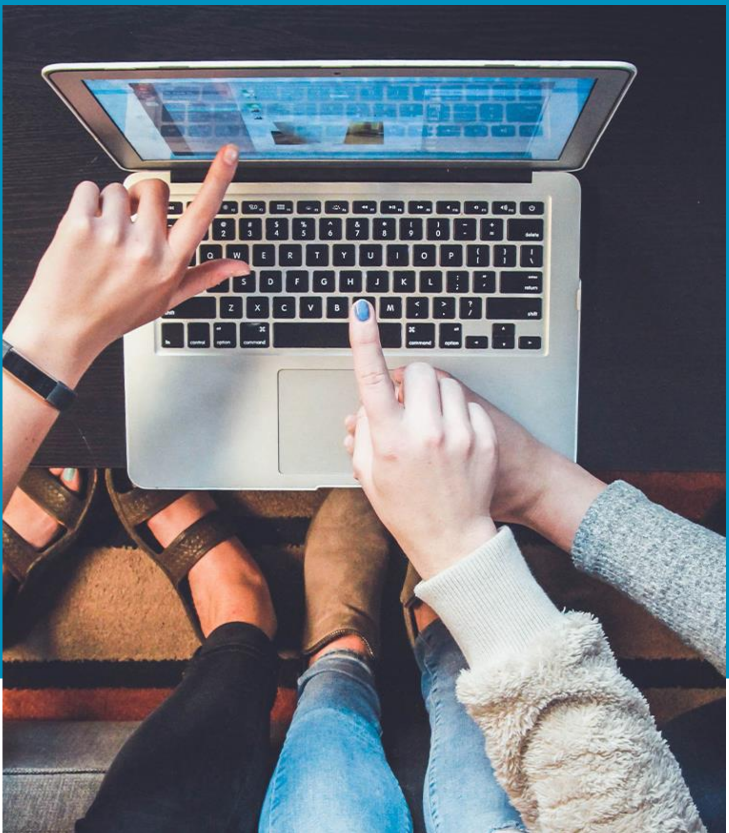
Patches Notes

ADOBE PLUGS CRITICAL PHOTOSHOP SECURITY FLAWS

- Adobe has issued a security alert regarding two critical security flaws in its renowned Photoshop image manipulation product.
- Adobe also issued warnings with updates for severe security flaws in Adobe Media Encoder (code execution, critical), as well as multiple major security flaws in Adobe Bridge and Adobe Captivate.

CISCO VULNERABILITY IN END-OF-LIFE VPN ROUTERS DECLINED

- An critical vulnerability in Universal Plug-and-Play (UPnP) service of multiple small business VPN routers will not be patched because the devices have reached end-of-life.
- Unauthenticated attackers can exploit it to restart vulnerable devices or execute arbitrary code remotely as the root user on the underlying operating system.



MACOS 11'S HIDDEN SECURITY IMPROVEMENTS

- New security features in macOS i.e.: (i) Pointer Authentication Codes (PAC), (ii) Device isolation, (iii) Write XOR Execute (W^X), and (iv) Signed System Volume (SSV)
- SDK versions security holes were fixed in the case for fcntl(2) command F_SETSIZE.

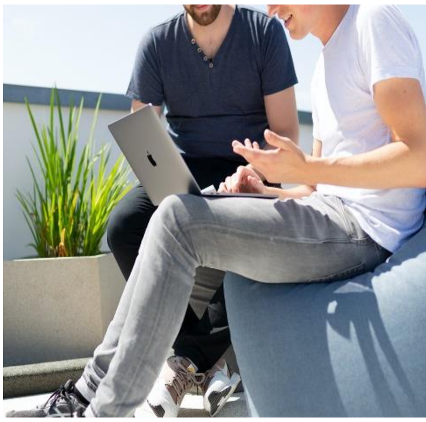
CYBER ATTACKS

CHASE BANK ACCIDENTALLY LEAKED CUSTOMER INFO TO OTHER CUSTOMERS

- Chase Bank has acknowledged the existence of a technical flaw on its online banking website and app that allowed client banking information to be accidentally leaked to other customers.
- Customers' personal information, such as statements, transaction lists, names, and account numbers, could have been accessible to other Chase banking members.

EDUCATION GIANT PEARSON FINED $1M FOR DOWNPLAYING DATA BREACH

- Pearson agreed to pay a $1 million civil money penalty to settle claims that it tried to conceal and downplay a 2018 data breach in the United States that resulted in the loss of "student data and administrator log-in credentials of 13,000 school, district, and university customer accounts."
- Customers' personal information, such as statements, transaction lists, names, and account numbers, could have been accessible to other Chase banking members.



IT GIANT ACCENTURE HIT BY LOCKBIT RANSOMWARE; HACKERS THREATEN TO LEAK DATA

- Accenture, a global IT consulting firm, has become the latest victim of the LockBit ransomware group.
- LockBit, like its now-defunct DarkSide and REvil counterparts, uses a ransomware-as-a-service (RaaS) model, enlisting the help of other cybercriminals (referred to as affiliates) to carry out the attack on its behalf, with the proceeds split between the criminal entity...

T-MOBILE DATA BREACH IS ONE YOU CAN'T IGNORE

- While the hacker first claimed that data from 100 million users had been compromised, the vast majority of those affected were not current T-Mobile customers at all.
- The information of around 48 million users was taken, including their full names, dates of birth, social security numbers, and driver's licence numbers. An further 850,000 prepaid customers—those who pre-fund their accounts—had their names, phone numbers,

Malware and Vulnerabilities

XSS BUG IN SEOPRESS WORDPRESS PLUGIN ALLOWS SITE TAKEOVER

- The SEOPress WordPress plugin contains a stored cross-site scripting (XSS) vulnerability that might allow attackers to insert arbitrary web programmes into websites.
- When a user entered the ‘All Posts' page, these web scripts would run. Cross-site scripting flaws like this one can lead to a range of malicious behaviours, including the establishment of new administrative accounts, webshell injection,

HUNDREDS OF HIGH-TRAFFIC WEB DOMAINS VULNERABLE TO SAME-SITE ATTACKS

- Related-domain assaults are an underappreciated issue that can allow hostile actors to bypass many effective website protection solutions.
- Dangling DNS records, records in a domain's authoritative DNS servers that refer to expired resources that can be acquired by an adversary, are a critical vulnerability vector.

UNPATCHED REMOTE HACKING FLAW DISCLOSED IN FORTINET'S FORTIWEB WAF

- A flaw in Fortinet's web application firewall (WAF) has been identified, allowing attackers to execute arbitrary instructions on devices and servers running the protection software.
- Because the vulnerability is only available to authenticated persons, an attacker would need to get the administrator's credentials before launching an attack.

MULTIPLE FLAWS AFFECTING REALTEK WI-FI SDKS IMPACT NEARLY A MILLION IOT DEVICES

- Realtek, a Taiwanese chipmaker, has issued a security alert for three software development kits (SDKs) that come with its WiFi modules, which are utilised in nearly 200 IoT devices from at least 65 vendors.
- Residential gateways, travel routers, WiFi repeaters, IP cameras, smart lightning gateways, and even connected toys from a variety of brands are among the products that will be impacted.

CYBER TECH

FACEBOOK ADDS END-TO-END ENCRYPTION FOR AUDIO AND VIDEO CALLS IN MESSENGER

- Facebook announced on Friday that it is expanding end-to-end encryption (E2EE) for audio and video conversations in Messenger, as well as testing a new opt-in setting that would enable E2EE for Instagram DMs.

- In addition, Instagram is scheduled to launch a limited test in a few countries that allows users to opt-in to end-to-end encrypted messages and calls for one-on-one chats.

MICROSOFT TEAMS WILL ALERT USERS OF INCOMING SPAM CALLS

- The Microsoft 365 Teams collaboration platform is getting a spam call notification function. When the new capability is available, Microsoft Teams will notify Office 365 subscribers if they receive what seems to be spam calls.

- Users can still answer or reject the call, and all'spam likely' calls will be recorded in the call history list (regardless of whether they were answered or rejected).

WINDOWS 11 GETS NEW VERSIONS OF SNIPPING TOOL, MAIL, AND CALCULATOR

- With updated versions of the Calculator, Mail and Calendar, and Snipping Tool apps, Microsoft is releasing its first Windows 11 app updates.

- Both the traditional Snipping Tool and Snip & Sketch programmes have been replaced in Windows 11 by a new Snipping Tool app that combines the finest features of both in the next generation of screen capture for Windows.

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.

SECURITY ORCHESTRATION AUTOMATION & RESPONSE

Security Orchestration, Automation, and Response solutions bring out the best in cybersecurity by efficiently combining automation, orchestration & threat data collection from multiple sources and automatically responding to low level security events without human assistance. The goal of using a SAOR stack is to improve the efficiency of physical & digital security operations and to have a single and comprehensive incident response platform.

Infopercept
SECURE • OPTIMIZE • STRENGTHEN
+91 98988 57117
sos@infopercept.com
www.infopercept.com

INVINSENSE™
Attacktical Cybersecurity Sense