INVINSENSE™
Attacktical Cybersecurity Sense

Infopercept

INVINSENSE SECURITY AWARENESS BULLETIN

ISSUE -17 Jan 2022

Contents

Patches Notes

LATEST WORDPRESS SECURITY RELEASE FIXES XSS, SQL INJECTION BUGS

- WordPress's developers have released a security-focused update that fixes four major security problems in the content management system.
- WordPress 5.8.3 explicitly addresses cross-site scripting (XSS) and SQL injection vulnerabilities in WordPress versions 3.7 to 5.8.

INDIAN ACADEMIC BOOKSELLER OSWAAL BOOKS FIXES ALLEGED RCE AND OTHER SERIOUS VULNERABILITIES WITH SHOPIFY RELAUNCH

- According to a security researcher, flaws in the e-commerce domain of Indian bookseller Oswaal Books could have allowed attackers to take control of the website.
- By gaining control of the administrator account via SQL injection, the researcher was able to perform RCE, bypass OTP authentication, and discover a CSRF bug.

VMWARE PATCHES IMPORTANT BUG AFFECTING ESXI, WORKSTATION AND FUSION PRODUCTS

- VMWare has released updates for Workstation, Fusion, and ESXi products to address a "important" security vulnerability that a threat actor could exploit to take control of affected systems.
- The problem is related to a heap-overflow vulnerability — CVE-2021-22045 (CVSS score: 7.7) — that, if successfully exploited, allows arbitrary code to be executed.

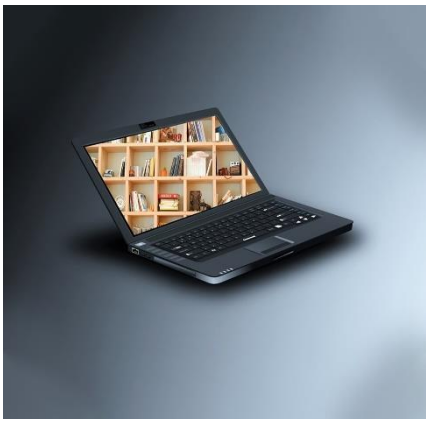
CYBER ATTACKS

INSECURE AMAZON S3 BUCKET EXPOSED PERSONAL DATA ON 500,000 GHANAIAN

- Researchers at vpnMentor claim to have discovered a trove of unencrypted data related to Ghana's National Service Secretariat (NSS) in an Amazon Web Services storage silo (AWS).
- Some of the 3 million files related to NSS's work and stored on an AWS S3 bucket were password protected, but many were not – an oversight that exposed the personal information of an estimated 500,000-600,000 people till 2021.

URL PARSING BUGS ALLOW DOS, RCE, SPOOFING & MORE

- Dangerous security flaws caused by widespread inconsistencies among 16 popular third-party URL-parsing libraries could have a wide-ranging impact on web applications.
- The flaws were discovered in third-party web packages written in various languages, and they could have been imported into thousands of different projects, similar to Log4Shell and other software-supply chain threats.



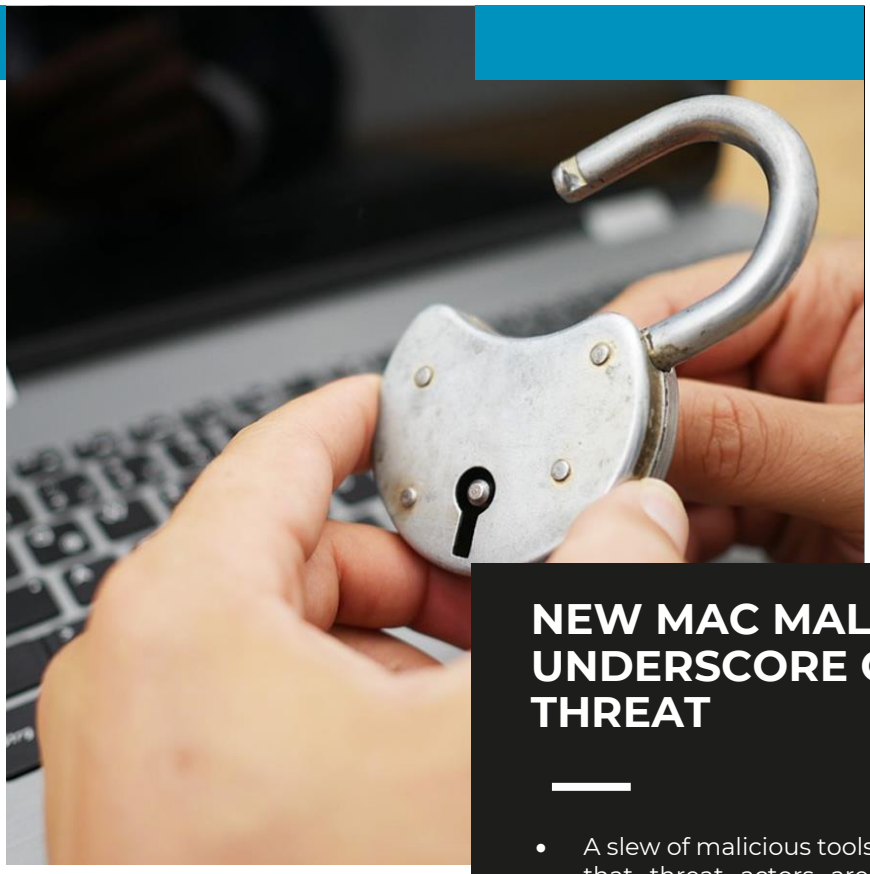
DATA BREACH: BROWARD HEALTH WARNS 1.3 MILLION PATIENTS, STAFF OF 'MEDICAL IDENTITY THEFT'

- The Broward Health hospital system notified more than 1.3 million patients and staff members this weekend that their personal information was compromised in a data breach that began on October 15.
- People whose information was compromised are now vulnerable to medical identity theft, which occurs when someone uses another person's name and information to obtain medical services or fraudulently bill for medical services.

Malware and Vulnerabilities

APPLE IPHONE MALWARE TACTIC CAUSES FAKE SHUTDOWNS TO ENABLE SPYING

- The 'NoReboot' technique is the pinnacle of iPhone malware persistence, preventing reboots and allowing remote attackers to do anything on the device while remaining completely undetected.
- Because an infected user may believe "that the phone has been powered off.



NEW MAC MALWARE SAMPLES UNDERSCORE GROWING THREAT

- A slew of malicious tools that surfaced last year suggested that threat actors are becoming more serious about attacking Apple's macOS and iOS environments.
- A small number of malware samples discovered in 2021 demonstrated that, while Apple's technologies are less vulnerable to attack and compromise than Windows systems, they are not immune.

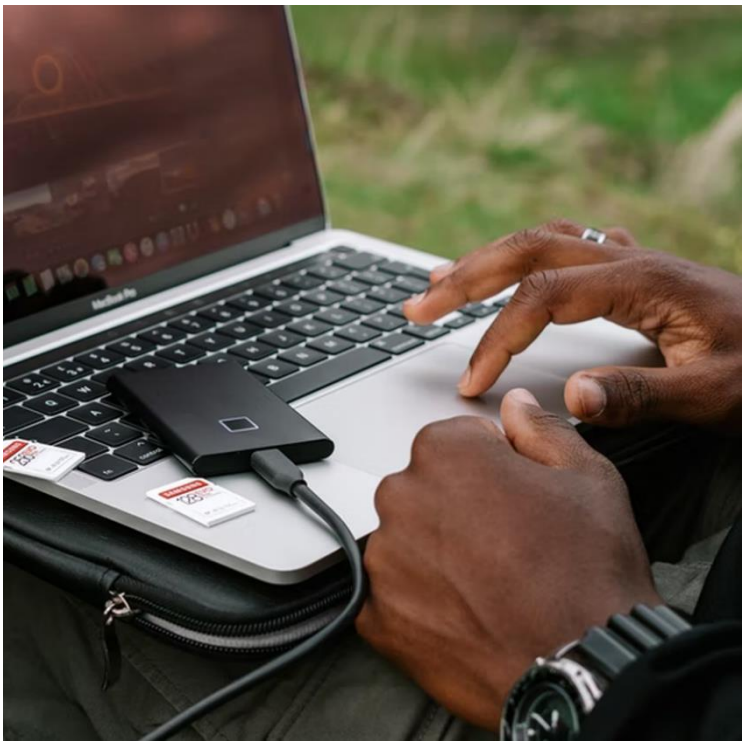
SONICWALL: Y2K22 BUG HITS EMAIL SECURITY, FIREWALL PRODUCTS

- SonicWall confirmed today that the Y2K22 bug has affected some of its Email Security and firewall products, causing message log updates and junk box failures beginning January 1st, 2022.
- Users will also be unable to trace incoming/outgoing emails using the message logs because they are no longer updated.

CYBER TECH

REPORT: DDOS ATTACKS INCREASING YEAR ON YEAR AS CYBERCRIMINALS DEMAND EXTORTIONATE PAYOUTS

- According to Cloudflare, a new botnet known as the Meris botnet appeared in mid-2021 and was the source of many high-volume application-layer DDoS attacks.
- Application-layer DDoS attacks aim to disrupt the operation of a targeted organization's web server by flooding it with bogus requests, causing it to slow down or (worst yet) crash.



RESEARCHERS DISCOVER LOG4J-LIKE FLAW IN H2 DATABASE CONSOLE

- In the console of the immensely popular Java SQL database, H2 Database Engine, a vulnerability with the same fundamental cause as the well-known Log4j bug has been addressed.
- According to a GitHub security advisory provided by the H2 maintainers on January 5, the flaw (CVE-2021-42392) "allows loading of custom classes from remote servers via JNDI.

NEW WAYS TO HIDE MALWARE INSIDE SSD FIRMWARE DISCOVERED

- A new set of assaults against Solid-State Drives has been devised by Korean researchers (SSDs). These attacks allow malware to be deployed in places where security solutions and users are unable to reach it.
- The assaults target drives with flex capacity features and hidden sections on the device known as over-provisioning areas, which are used by SSD manufacturers for performance improvement on NAND flash storage devices.

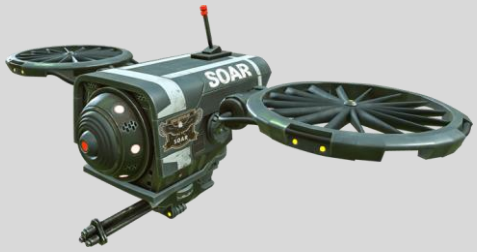
Infopercept

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 conducts the following steps to implement SOAR;

- Threat and Vulnerability Management
- Security Incident Response
- Incident Report Automation
- Security Operations Automation

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

INYINSENSE™
Attacktical Cybersecurity Sense