INVINSENSE™
Attacktical Cybersecurity Sense

Infopercept

INVINSENSE SECURITY AWARENESS BULLETIN

ISSUE -20 Dec 2021

Contents

Patches Notes

SONICWALL URGES CUSTOMERS TO IMMEDIATELY PATCH CRITICAL SMA 100 FLAWS

- Following the revelation of various security vulnerabilities that might be exploited by a remote attacker to take complete control of an affected machine, network security provider SonicWall is encouraging users to update their SMA 100 series appliances to the current version.
- SMA 200, 210, 400, 410, and 500v products running versions 9.0.0.11-31sv and earlier, 10.2.0.8-37sv, 10.2.1.1-19sv, 10.2.1.2-24sv and prior are affected by the issues. The security flaws were discovered and reported by security experts Jake Baines (Rapid7)

MICROSOFT ISSUES WINDOWS UPDATE TO PATCH 0-DAY USED TO SPREAD EMOTET MALWARE

- Microsoft has released Patch Tuesday updates to address multiple security flaws in Windows and other software, including one actively exploited flaw that is being used to deliver Emotet, TrickBot, or Bazaloader malware payloads.
- According to the Zero Day Initiative, the latest monthly release for December fixes a total of 67 flaws, bringing the company's total number of bugs patched this year to 887. Seven of the 67 flaws are rated Critical, and 60 are rated Important, with five of the issues being publicly known at the time of release.

UPDATE GOOGLE CHROME TO PATCH NEW ZERO-DAY EXPLOIT DETECTED IN THE WILD

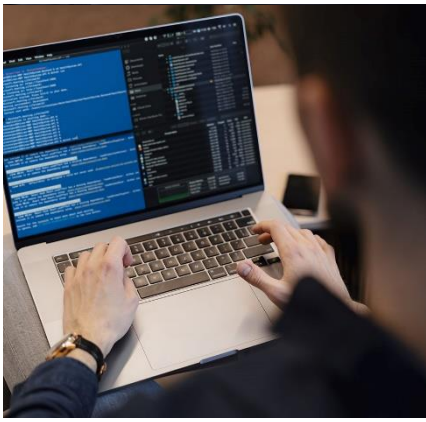
- Google has released patches for five security flaws in its Chrome web browser, including one that it claims is being exploited in the wild, making it the 17th vulnerability to be revealed since the beginning of the year.
- The issue, which has been assigned the number CVE-2021-4102, is a use-after-free bug in the V8 JavaScript and WebAssembly engine that might result in serious effects ranging from data corruption to the execution of arbitrary code.

CYBER ATTACKS

1.6 million WordPress sites targeted in the last couple of days

- "On December 9, 2021, the Threat Intelligence team saw a significant increase in attacks targeting vulnerabilities that allow attackers to alter arbitrary parameters on susceptible sites," says the report. This prompted an inquiry, which resulted in the discovery of a live attack aimed at over a million WordPress sites." according to a Wordfence blog article. "Over the past 36 hours, the Wordfence network has blocked over 13.7 million attacks across over 1.6 million sites, coming from over 16,000 distinct IP addresses, targeting four different plugins...

MICROSOFT VANCOUVER LEAKING WEBSITE CREDENTIALS VIA OVERLOOKED DS_STORE FILE



- The metadata on the file directed the researchers to several WordPress database dumps containing multiple administrator usernames and email addresses, as well as the hashed password for the Microsoft Vancouver website.
- Leaving DS STORE files on remote web servers is risky because they expose their folder structure, potentially leaking sensitive or confidential data. This is precisely what happened with the lingering DS STORE file on the Microsoft Vancouver web server.

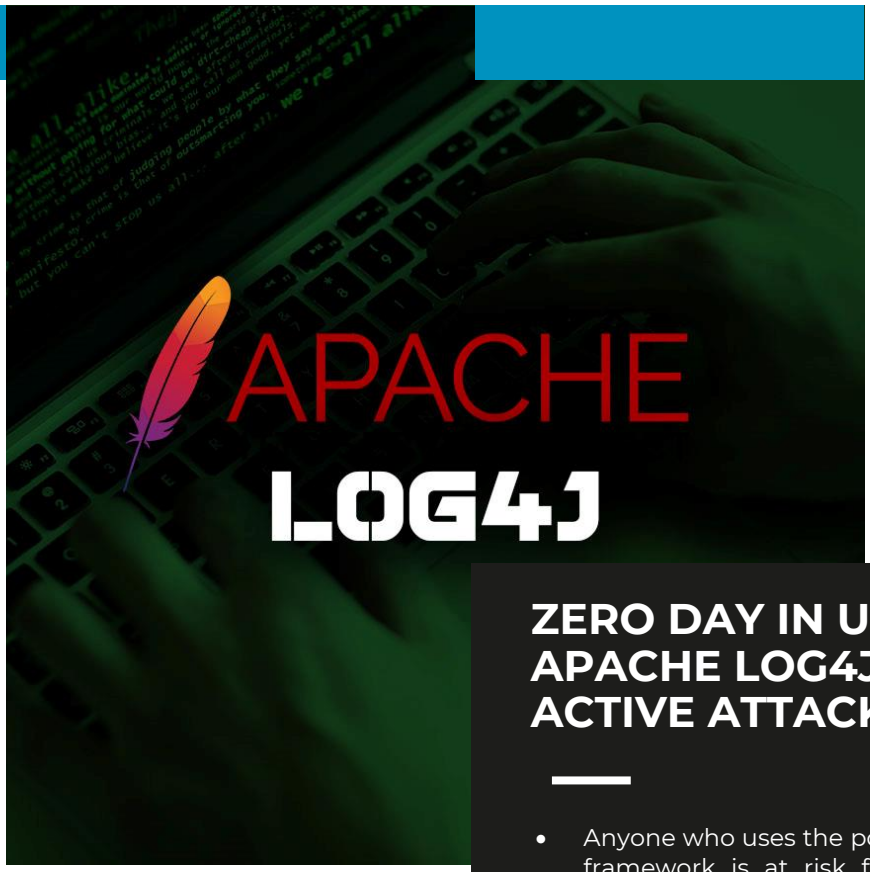
HACKERS USING MALICIOUS IIS SERVER MODULE TO STEAL MICROSOFT EXCHANGE CREDENTIALS

- On Microsoft Exchange Outlook Web Access servers, malicious actors are distributing a previously unknown malware, an Internet Information Services (IIS) webserver module branded "Owowa," with the objective of stealing credentials and enabling remote command execution.
- According to Kaspersky researchers Paul Rascagneres and Pierre Delcher, "Owowa is a C#-developed.NET v4.0 assembly that is designed to be loaded as a module within an IIS web server that also exposes Exchange's Outlook Web Access (OWA)."

Malware and Vulnerabilities

BLACKCAT: A NEW RUST-BASED RANSOMWARE MALWARE SPOTTED IN THE WILD

- MalwareHunterTeam revealed the ransomware, called BlackCat. In a series of tweets revealing the file-encrypting malware, the researchers stated, "Victims can pay using Bitcoin or Monero." "It also appears that they are providing credentials to middlemen" for the purposes of negotiations.



ZERO DAY IN UBIQUITOUS APACHE LOG4J TOOL UNDER ACTIVE ATTACK

- Anyone who uses the popular open-source Apache Struts framework is at risk from the Log4Shell vulnerability, which might result in a "little internet meltdown soonish."
- An excruciatingly easy-to-exploit bug in the widely used Java logging library Apache Log4j might allow unauthenticated remote code execution (RCE) and complete server takeover, and it's already been exploited.

MICROSOFT DETAILS BUILDING BLOCKS OF WIDELY ACTIVE QAKBOT BANKING TROJAN

- The Microsoft 365 Defender Threat Intelligence Team dubbed Qakbot a "customizable chameleon that adapts to suit the needs of the multiple threat actor groups that use it," which will aid in proactively detecting and blocking the threat.
- the modular malware — like TrickBot — has evolved from its early roots as a banking trojan to become a Swiss Army knife capable of data exfiltration and acting as a delivery mechanism for second stage payloads such as ransomware.

CYBER TECH

OWASP MODSECURITY CORE RULE SET SANDBOX LAUNCHED TO HELP SECURITY RESEARCHERS TEST NEW CVES

- Security researchers can now test payloads against the OWASP ModSecurity Core Rule Set with a new sandbox released by the project maintainers. The CRS is a set of generic attack detection rules for use with ModSecurity or compatible web application firewalls. A sandbox API was created following "regular" conversations with security researchers about how they can use the CRS. The code behind the CRS sandbox was inspired by a meeting with PortSwigger's James Kettle and Gareth Hayes at AppSec Amsterdam in 2019.

- The sandbox, which is free to use, is hosted on AWS and collects logs, though the IP addresses will be anonymized. Plans for future features include the ability to create a users' 'hall of fame' and share information on payloads with others.

AWS LAUNCHES ITS SECOND TOP SECRET REGION

- AWS Top Secret-West, Amazon Web Services' second Top Secret area, was launched on Tuesday. Customers in the defence, intelligence, and national security sectors will benefit from the new area, which is accredited to execute workloads classified as Top Secret in the United States.

- AWS Top Secret-East, Amazon's first Top Secret region, was launched in 2014, making it the first air-gapped commercial cloud to serve classified workloads.

HOW TO USE THE IPHONE'S NEW APP PRIVACY REPORT

- If you're an iPhone user, you can now learn more about how often your apps access your data (for example, your location or your microphone). The App Privacy Report, which debuted with iOS 15.2, now shows you each app's web activity and the domains to which it is linked.

- The feature is disabled by default, however it's easy to enable if your phone has been upgraded to iOS 15.2: To get the App Privacy Report, go to Settings > Privacy > App Privacy Report (which will be at the bottom of the screen) "Turn On App Privacy Report" should be selected.

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

INVINSENSE™
Attacktical Cybersecurity Sense