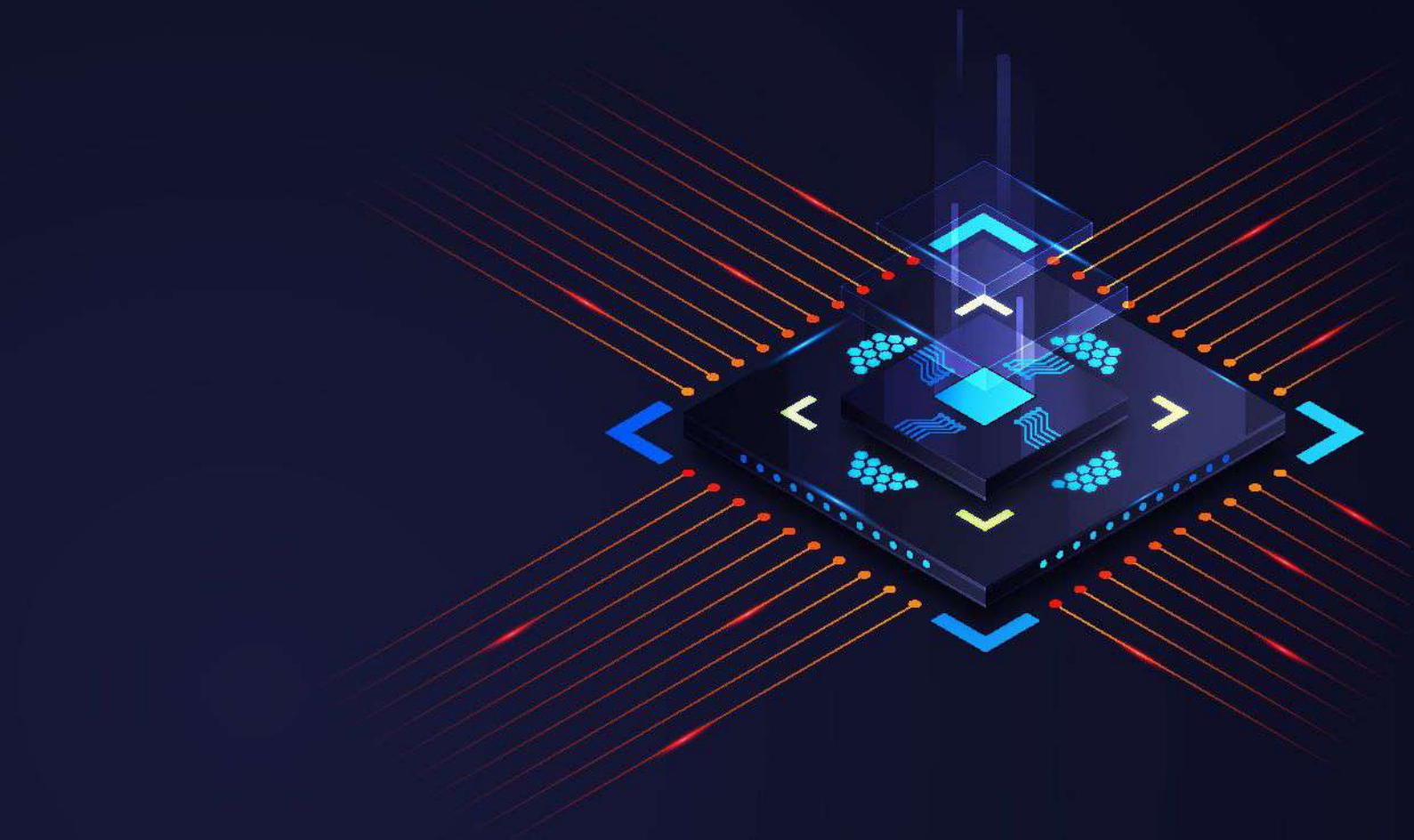
CyberPeace
Foundation

ADVISORY REPORT ON

Zoom Screen Sharing Bug

(CVE-2021-28133)



Advisory report on
Zoom Screen Sharing Bug (CVE-2021-28133)

Date : 01 April 2021
Problem ID & Name : Zoom Screen Sharing Bug (CVE-2021-28133)
Severity : Medium

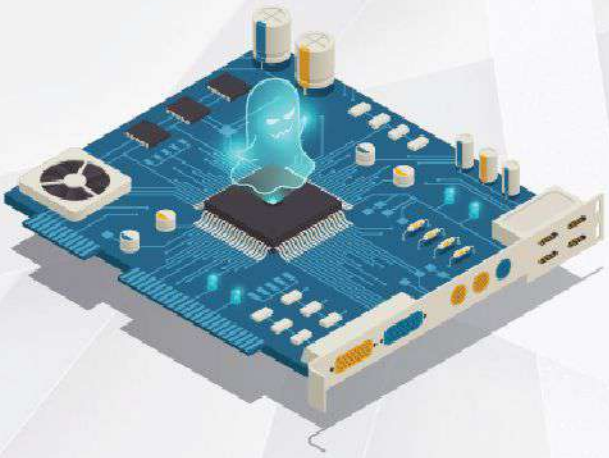
Executive summary :

A newfound glitch in Zoom's screen sharing element can coincidentally release touchy data to different participants during a call. Followed as CVE-2021-28133, the unpatched security vulnerability makes it conceivable to uncover materials of utilisation that are not shared, yet just momentarily, in this manner making it harder to abuse it in nature.

It merits calling attention to the screen sharing usefulness of Zoom which allows clients to share a whole work area or telephone screen, or limit sharing to at least one explicit application, or a part of a screen. The issue originates when a subsequent application that is overplayed on top of a generally shared application uncovers it's substance for a brief time. When a Zoom client shares a particular application window through the '**share screen**' mode, other gathering members can momentarily see the gesture of other application windows which were not unequivocally shared,. The images of not shared application windows can, for example, be seen for a brief timeframe by different clients when those windows overlay the common application window and get into the centre. The defect was tried on adaptations inversion of 5.4.3 and 5.5.4 across the two Windows and Linux users. The absence of a fix followed for three months could be ascribed to a limited extent to the trouble in misusing the vulnerability.

Now, what is CVE-2021-28133 ?

Zoom through 5.5.4 version permits assailants to peruse private data on a member's screen, even though the member never endeavoured to share the personal tabs or folders of their screen. At the point when a client shares a particular application window through the share screen, other gathered members can momentarily see the gesture of other application windows that were unequivocally not shared. An assailant can utilize a different screen-recorder application, unsupported by Zoom, to save all such records for later usage and investigation.



CyberPeace Foundation

Dependent on the accidentally shared information, this short openness of screen might be a pretty much extreme security issue. Beneath is an example of the entire show as :

- Let's suppose in this assault situation, the two clients A and B are in the same Zoom meeting and A shares her internet browser window using the "share screen" application.

- B records her entire work area screen utilising a screen recorder programming, for example, Simple Screen Recorder or any other 3rd party application. Between showing various things on her internet browser window, A utilises another application whose window ends up overlaying the internet browser window.

- The content of another application window, which is unequivocally not conveyed to B, can now and then temporarily be seen by B. When watching the recording, B can stop the video and can unintentionally or intentionally see the accidentally shared application window content from A.

With the COVID pandemic more associations bend by going online and remote working over a year and consequently different web conferencing stages such as Zoom and other video conferencing platforms became popular. Zoom has been wrestling with different security and protection issues, including aggressors capturing the web gatherings in a thing called Zoom bombing assaults. Other security issues have become visible in Zoom's foundation during the year, for example, one that might have permitted assailants to break private meeting passwords and sneak in on video meetings.

As per mitigation and recommendation :

- In order to minimise risks of getting compromised, Android users are advised to install a security solution and to limit their downloads to vendor-recommended application stores or completely ignore the use of Zoom app by all means when the security update or patch wasn't published by the platform creator itself.

- Perform standard reinforcements of all basic data to restrict the effect of information or frame-work misfortune and to help speed up the restoration cycle. Preferably, this information should be kept on a different gadget, and reinforcements should be kept away disconnected.

- While screen sharing does not open entire tabs and folders for display rather than displays the required tab or folder which is necessary to display. Protect passcodes and meeting ID and share the credentials when required rather than sharing it in advance.

- It is recommended to keep updated on all the apps on the device.

Reference

- https://threatpost.com/zoom-glitch-leaks-data/164876/#:~:text=The%20flaw%20(CVE%2D2021%2D,in%20a%20Zoom%20conferencing%20call
- https://twitter.com/dsci_tir/status/1374330727274213379?s=21
- https://nvd.nist.gov/vuln/detail/CVE-2021-28133
- https://www.tenable.com/cve/CVE-2021-28133
- https://www.cybersecurity-help.cz/vdb/SB2021032221
- http://seclists.org/fulldisclosure/2021/Mar/48
- https://thehackernews.com/2021/03/new-zoom-screen-sharing-bug-lets-other.html
- https://www.syss.de/fileadmin/dokumente/Publikationen/Advisories/SYSS-2020-044.txt
- https://www.syss.de/pentest-blog/syss-2020-044-sicherheitsproblem-in-screen-sharing-funktionalitaet-von-zoom-cve-2021-28133
- https://www.youtube.com/watch?v=SonmmgQlLzg
- https://zoom.us/trust/security/security-bulletin

Revision Notes :

VERSION	DESCRIPTION	SECTION	STATUS	DATE
1.0	Initial Public Release	---	Final	01/04/21

Issued by :

Research Wing, CyberPeace Foundation
Research Wing, Autobot Infosec Private Ltd.

CyberPeace Foundation

CyberPeace
Foundation

"IN PURSUIT OF CYBERPEACE"

www.cyberpeace.org | secretariat@cyberpeace.net | +91 823 5058 865

Secretariat: B-55, MIG, Harmu Housing Colony, Birsa Munda Rajpath
Ranchi, Jharkhand 834002

Delhi: L29 - L34, First Floor, Connaught Place, New Delhi, Delhi 110001

/cyberpeacefoundation /cyberpeacengo /cyberpeacefoundation