Advisory Alert

Alert Number: AAA20211117 **Date:** November 17, 2021

Document Classification Level : Public Circulation Permitted | Public

Information Classification Level : TLP: WHITE

Overview

Product	Severity	Vulnerability
Zoom	**High**	Multiple Vulnerabilities

Description

Affected Product	**Zoom**
Severity	**High**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2021-34422, CVE-2021-34417, CVE-2021-34420, CVE-2021-34418, CVE-2021-34421, CVE-2021-34419)
Description	Zoom has released Security Updates addressing multiple vulnerabilities that exist with Zoom products. **CVE-2021-34422 -** When checking the name of a file uploaded to a team folder in the Keybase Client, a path traversal vulnerability exists. **CVE-2021-34417 -** The network proxy page on the web portal fails to verify input sent in requests to configure the network proxy password. **CVE-2021-34420 -** The signature of files with the .msi, .ps1, and .bat extensions is not properly verified by the Zoom Client for Meetings. **CVE-2021-34418 -** The web console's login service fails to validate that a NULL byte was sent while authenticating. **CVE-2021-34421 -** When the receiving user places the chat session in the background while the sending user explodes the messages, the Keybase Client for Android and the Keybase Client for iOS fail to properly delete exploded messages initiated by the user. **CVE-2021-34419 -** When sending a remote-control request to a user in the process of in-meeting screen sharing, there is an HTML injection flaw in the Zoom Client for Meetings for Ubuntu Linux.
Affected Products	Keybase Client for Windows before version 5.7.0 All Keybase Client for Android before version 5.8.0 All Keybase Client for iOS before version 5.8.0 All Zoom Client for Meetings for Windows before version 5.5.4 Zoom Client for Meetings for Ubuntu Linux before version 5.1.0 Zoom On-Premise Meeting Connector Controller before version 4.6.239.20200613 Zoom On-Premise Meeting Connector MMR before version 4.6.239.20200613 Zoom On-Premise Recording Connector before version 3.8.42.20200905 Zoom On-Premise Virtual Room Connector before version 4.4.6344.20200612 Zoom On-Premise Virtual Room Connector Load Balancer before version 2.5.5492.20200616 Zoom On-Premise Meeting Connector Controller before version 4.6.365.20210703 Zoom On-Premise Meeting Connector MMR before version 4.6.365.20210703 Zoom On-Premise Recording Connector before version 3.8.45.20210703 Zoom On-Premise Virtual Room Connector before version 4.4.6868.20210703 Zoom On-Premise Virtual Room Connector Load Balancer before version 2.5.5496.20210703
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://explore.zoom.us/en/trust/security/security-bulletin/?filter-cve=CVE-2021-34422%2CCVE-2021-34421%2CCVE-2021-34420%2CCVE-2021-34419%2CCVE-2021-34418%2CCVE-2021-34417&filter=&keywords=

Disclaimer

The information provided herein is on "as is" basis, without warranty of any kind. FinCSIRT highly recommend to follow the company policies and procedures when applying the necessary patches with thorough testing and ensuring proper roll-back capabilities exists.