Hive Pro

THREAT ADVISORY

Have you updated your Zoom meeting?

TA202152

Threat Level AMBER

Publish Date – Nov 30, 2021

Two Critical vulnerabilities have been found in Zoom products. These vulnerabilities were discovered by Natalie Silvanovich, a researcher from Google Project Zero.

The first vulnerability, CVE-2021-34423 is a high severity and a buffer overflow vulnerability. This could allow an attacker to crash the service or application or exploit the vulnerability by executing an arbitrary code.

The second vulnerability, CVE-2021-34424 is a medium severity and a memory corruption vulnerability. This flaw could be used to get access to arbitrary parts of the product's memory.

Both these vulnerabilities can be fixed by updating Zoom products to their latest versions.

Vulnerability Details

CVE ID	Affected Products	Affected CPE	Vulnerability Name	CWE ID
CVE-2021-34423	Zoom Client for Meetings (for Android, iOS, Linux, macOS, and Windows) before version 5.8.4 Zoom Client for Meetings for Blackberry (for Android and iOS) before version 5.8.1 Zoom Client for Meetings for intune (for Android and iOS) before version 5.8.4 Zoom Client for Meetings for Chrome OS before version 5.0.1 Zoom Rooms for Conference Room (for Android, AndroidBali, macOS, and Windows) before version 5.8.3 Controllers for Zoom Rooms (for Android, iOS, and Windows) before version 5.8.3 Zoom VDI before version 5.8.4 Zoom Meeting SDK for Android before version 5.7.6.1922 Zoom Meeting SDK for iOS before version 5.7.6.1082 Zoom Meeting SDK for macOS before version 5.7.6.1340 Zoom Meeting SDK for Windows before version 5.7.6.1081 Zoom Video SDK (for Android, iOS, macOS, and Windows) before version 1.1.2 Zoom On-Premise Meeting Connector Controller before version 4.8.12.20211115 Zoom On-Premise Meeting Connector MMR before version 4.8.12.20211115 Zoom On-Premise Recording Connector before version 5.1.0.65.20211116 Zoom On-Premise Virtual Room Connector before version 4.4.7266.20211117 Zoom On-Premise Virtual Room Connector Load Balancer before version 2.5.5692.20211117 Zoom Hybrid Zproxy before version 1.0.1058.20211116 Zoom Hybrid MMR before version 4.6.20211116.131_x86-64	cpe:2.3:a:zoom:client_for_meetings:*:*:*:*:*:*:*:*, cpe:2.3:a:zoom:rooms_for_conference_room:*:*:*:*:*:*:*:*, cpe:2.3:a:zoom:controllers_for_zoom_rooms:*:*:*:*:*:*:*:*, cpe:2.3:a:zoom:vdi:*:*:*:*:*:*:*:*, cpe:2.3:a:zoom:sdk:*:*:*:*:*:*:*:*, cpe:2.3:a:zoom:meeting_sdk:*:*:*:*:*:*:*:*, cpe:2.3:a:zoom:video_sdk:*:*:*:*:*:*:*:*, cpe:2.3:a:zoom:on-premise_meeting_connector_controller:*:*:*:*:*:*:*:*, cpe:2.3:a:zoom:on-premise_meeting_connector_mmr:*:*:*:*:*:*:*:*, cpe:2.3:a:zoom:on-premise_recording_connector:*:*:*:*:*:*:*:*, cpe:2.3:a:zoom:on-premise_virtual_room_connector:*:*:*:*:*:*:*:*, cpe:2.3:a:zoom:on-premise_virtual_room_connector_load_balancer:*:*:*:*:*:*:*:*, cpe:2.3:a:zoom:hybrid_zproxy:*:*:*:*:*:*:*:*, cpe:2.3:a:zoom:hybrid_mmr:*:*:*:*:*:*:*:*	Buffer overflow in Zoom Client and other products	CWE-120
CVE-2021-34424			Process memory exposure in Zoom Client and other products	CWE-371

References

https://securityaffairs.co/wordpress/125122/security/video-conferencing-software-zoom-flaws.html
https://explore.zoom.us/en/trust/security/security-bulletin/