Vulnerability in Multiple Zoom Products

Severity Level: High

Components Affected

- Zoom Desktop Client for Windows before version 5.16.5
- Zoom VDI Client for Windows before version 5.16.10 (excluding 5.14.14 and 5.15.12)
- Zoom Rooms Client for Windows before version 5.17.0
- Zoom Meeting SDK for Windows before version 5.16.5

Overview

Improper input validation in multiple zoom products were identified. That may allow an unauthenticated user to conduct an escalation of privilege via network access.

Description

The manipulation with an unknown input leads to an input validation vulnerability found in multiple Zoom Products. The product receives input or data, but it does not validate or incorrectly validates that the input has the properties that are required to process the data safely and correctly. Which Impacts the confidentiality, integrity, and availability of these products. This vulnerability is tracked as CVE-2024-24691 and there are no other technical details publicly available yet.

Impact

- Elevation of Privilege
- Information Disclosure
- Injection attacks

Solution/ Workarounds

Before installation of the software, please visit the software vendor web-site for more details.
Apply fixes issued by the vendor:

- https://zoom.us/download

Reference

- https://vuldb.com/?id.253676
- https://www.zoom.com/en/trust/security-bulletin/ZSB-24008/

Disclaimer

The information provided herein is on an "as is" basis, without warranty of any kind.