**Security Advisory 2024-020**

# Critical Vulnerability in Zoom Products

***February 15, 2024 — v1.0***

**TLP:CLEAR**

*History:*

- *15/02/2024 — v1.0 – Initial publication*

## Summary

On February 13, 2024, Zoom released a security advisory [1] addressing one critical vulnerability. If exploited, this vulnerability allows an unauthenticated attacker to conduct privilege escalation on the target system via network access.

It is recommended applying updates as soon as possible [2].

## Technical Details

The vulnerability `CVE-2024-24691`, with a CVSS score of 9.6, is due to an improper input validation flaw that could allow an unauthenticated attacker to conduct privilege escalation on the target system over the network.

## Affected Products

This vulnerability impacts the following products:

- 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

## Recommendations

It is recommended applying updates as soon as possible [2].

## References

[1] https://www.zoom.com/en/trust/security-bulletin/ZSB-24008/

[2] https://zoom.us/download0