Executive Summary

Seven different Zoom vulnerabilities as of 13 February 2024 were identified in the video conferencing software. They affected a variety of Zoom clients, exposing users to a variety of potential security threats. Of the seven identified it should be noted that one was a critical security fix for a privilege escalation flaw. Through an improper input validation it was possible for an unauthenticated adversary to gain elevated privileges via network access.

Identified Vulnerabilities

CVE-2024-24691 (critical severity; CVSS 9.6): Improper input validation in Zoom Desktop Client for Windows, Zoom VDI Client for Windows, and Zoom Meeting SDK for Windows may allow an unauthenticated user to conduct an escalation of privilege via network access.

CVE-2024-24697 (high severity; CVSS 7.2): This vulnerability affected Zoom 32-bit Windows clients, letting an authenticated adversary gain elevated privileges via local access by exploiting an untrusted search path.

CVE-2024-24695 (medium severity; CVSS 6.8): Improper input validation in Zoom Desktop Client for Windows, Zoom VDI Client for Windows, and Zoom Meeting SDK for Windows may allow an authenticated user to conduct a disclosure of information via network access.

CVE-2024-24696 (medium severity; CVSS 6.8): Improper input validation with Zoom in-meeting chat could lead to information disclosure to an authenticated attacker via network access.

CVE-2024-24699 (medium severity; CVSS 6.5): Business login error with Zoom clients' in-meeting chat. Exploiting the flaw could result in information disclosure to an authenticated adversary.

CVE-2024-24690 (medium severity; CVSS 5.4): A denial of service vulnerability due to improper input validation.

CVE-2024-24698 (medium severity; CVSS 4.9): An information disclosure flaw that existed due to improper authentication, facilitating a privileged user with local access.

Recommendation

I recommend everyone consider updating their systems with the latest version of Zoom. They have already released patches addressing these vulnerabilities in multiple software releases. The latest version being 5.17.7 and by updating you are reducing your attack surface in an attenpt to avoid exploits of software that may leave us vulnerable.