Security Advisory 2022-038

Zoom Vulnerabilities

May 27, 2022 — v1.0

TLP:WHITE

History:

• 27/05/2022 — v1.0 – Initial publication

Summary

On the 17th of May 2022, Zoom released an advisory about two high vulnerabilities. They
are tracked as CVE-2022-22786 with a CVSS score of 7.5 and CVE-2022-22784 with a CVSS
score of 8.1. A successful exploitation of both of these vulnerabilities could be used in a more
sophisticated attack to trick a user into downgrading their Zoom client to a less secure version
and to forge XMPP messages from the server, respectively [1,2].

Technical Details

The CVE-2022-22786 affects the Zoom Client for Meetings for Windows and Zoom Rooms for
Conference Room for Windows which fail to properly check the installation version during the
update process.

The CVE-2022-22784 affects the Zoom Client for Meetings which fails to properly parse XML
stanzas in XMPP messages. This can allow a malicious user to break out of the current XMPP
message context and create a new message context to have the receiving user's client perform
a variety of actions.

Affected Products

CVE-2022-22786

• All Zoom Client for Meetings for Windows before version 5.10.0
• All Zoom Rooms for Conference Room for Windows before version 5.10.0

CVE-2022-22784

• Zoom Client for Meetings (for Android, iOS, Linux, macOS, and Windows) before version
  5.10.0
Recommendations

CERT-EU strongly recommends applying the available updates as soon as possible.

Workarounds

No workarounds are available.

References