NCA-250522-04	ADVISORY ON NEW ZOOM FLAWS

Overview

The popular video conferencing service Zoom is affected with four security vulnerabilities, CVE-2022-22784, CVE-2022-22785, CVE-2022-22786, and CVE-2022-22787, with severity levels ranging from 5.9 to 8.1. These vulnerabilities could be used to compromise another user over chat by sending engineered Extensible Messaging and Presence Protocol (XMPP) messages and executing malicious codes.

Impact

A successful attack could allow an attacker to force a vulnerable client to impersonate a Zoom user and connect to a malicious server, allowing for a number of attacks such as downgrade attacks, spoofing messages and sending control messages that are accepted as if they came from the server.

Technical Details

The Extensible messaging and Presence Protocol (XMPP) is a messaging protocol used by Zoom for its chat functionality. XMPP is used to send XML elements called stanzas through a stream connection to exchange messages.

- **CVE-2022-22784:** Improper XML Parsing in Zoom Client for Meetings which impacts Android, iOS, Linux, macOS, and Windows. This could be used to forge XMPP messages from the server.
- **CVE-2022-22785:** Improperly constrained session cookies in Zoom Client for Meetings which allow users to be easily spoofed.
- **CVE-2022-22786:** Package downgrade in Zoom Client for Meetings which specifically affects windows users. This issue could be used in a more sophisticated attack to trick a user into downgrading their Zoom client to a less secure version.
- **CVE-2022-22787:** Insufficient hostname validation during server switch in Zoom Client for Meetings. This vulnerability can be used to trick an unsuspecting user's client to connect to a malicious server when attempting to use Zoom services.

Preventive Measures

These mentioned vulnerabilities have all been resolved by Zoom. To prevent any potential threat emerging from active exploitation of these weaknesses, users should:

1. Update to the latest version of the application (5.10.0) as released by Zoom.
2. Download update only from Zoom's official page @ https://zoom.us/download

For further enquiries, please contact CERRT.NG through the following channels:
E-mail: cerrt@nitda.gov.ng
Phone:+2348178774580
Web: www.cerrt.ng