Computer Emergency Response Team of Mauritius
Ministry of Information Technology, Communication and Innovation

CERT-MU Vulnerability Note

Zoom for Windows Flaw Allows Attackers to Trigger Denial of Service Attacks

Vulnerability Note: VN-2025-09

Date of Issue: 09 July 2025

Severity Rating: High

Systems Affected:

The vulnerabilities affect a range of Zoom products for Windows, including

- Zoom Workplace for Windows before version 6.4.0
- Zoom Workplace VDI for Windows before version 6.3.10 (except 6.1.7 and 6.2.15)
- Zoom Rooms for Windows before version 6.4.0
- Zoom Rooms Controller for Windows before version 6.4.0
- Zoom Meeting SDK for Windows before version 6.4.0

Description

Security researchers have detected two significant vulnerabilities in Zoom Clients for Windows, exposing users to potential Denial of Service (DoS) attacks. The flaws, identified as classic buffer overflow vulnerabilities, could allow an authorized user to disrupt Zoom services via network access.

A buffer overflow occurs when a program writes more data to a buffer than it can hold. This can corrupt data, crash the application, or, in some cases, allow attackers to execute arbitrary code.

In the context of Zoom for Windows, these vulnerabilities could be exploited to trigger a DoS attack, rendering the service unavailable to legitimate users.

CVE Information

CVE-2025-49644
CVE-2025-46789

Workaround

Zoom recommends all users and administrators update their Windows clients to the latest versions available at the official Zoom download page.

More information about the update is available on:
https://www.zoom.com/en/trust/security-bulletin/zsb-25028/?ampDeviceId=cc0819b2-5b34-43a5-b1b4-d15337ff7c3f&SessionId=1751994983148

Postal address

Mauritian Computer Emergency Response Team (CERT-MU)
Ministry of Information Technology, Communication and Innovation
2nd Floor, Wing A,
Shri Atal Bihari Vajpayee Tower,
Cybercity Ebene,