ADV2026_156 Zoom Security Advisory (March 12ᵗʰ, 2026)

Zoom published security advisories highlighting vulnerabilities in the following products on March 10, 2026. It is recommended that you take the necessary precautions by ensuring your product is always updated.

- Zoom Meeting SDK for Windows – versions prior to 6.6.11
- Zoom Rooms for Windows – versions prior to 6.6.5
- Zoom Workplace for Windows – versions prior to 6.6.11
- Zoom Workplace VDI Client for Windows – versions prior to 6.4.17, 6.5.15 and 6.6.10

For more information on these updates, you can follow these URL:

- [Zoom Workplace for Windows - External Control of File Name or Path](#)
- [Zoom Clients for Windows - Improper Privilege Management](#)
- [Zoom Rooms for Windows - Improper Input Validation](#)
- [Zoom Workplace Clients for Windows - Improper Check](#)
- [Zoom Security Bulletins](#)

The Guyana National CIRT recommends that users and administrators review this update and apply it where necessary.

References

- Zoom Workplace for Windows - External Control of File Name or Path. (March 10, 2025). Retrieved from Zoom. https://www.zoom.com/en/trust/security-bulletin/zsb-26005/

- Zoom Clients for Windows - Improper Privilege Management. (March 10, 2025). Retrieved from Zoom. https://www.zoom.com/en/trust/security-bulletin/zsb-26004/

- Zoom Rooms for Windows - Improper Input Validation. (March 10, 2025). Retrieved from Zoom. https://www.zoom.com/en/trust/security-bulletin/zsb-26003/

- Zoom Workplace Clients for Windows - Improper Check. (March 10, 2025). Retrieved from Zoom. https://www.zoom.com/en/trust/security-bulletin/zsb-26002/

- Zoom Security Bulletins. (n.b.). Retrieved from Zoom. https://www.zoom.com/en/trust/security-bulletin/

- Zoom security advisory. (March 12, 2026). Retrieved from Canadian Centre for Cyber Security. https://www.cyber.gc.ca/en/alerts-advisories/zoom-security-advisory-av26-231