



NCSC-2025-0368

Kwetsbaarheden verholpen in Zoom Workplace en Zoom Clients

NCSC Advisory

Prioriteit: Normaal

Gepubliceerd op: 18-11-2025

TLP:WHITE

Toegestane verspreiding van TLP:WHITE

(Traffic Light Protocol)

Deze handreiking bevat het label TLP:WHITE en wordt door het NCSC verspreid. Het NCSC gebruikt het Traffic Light Protocol (TLP) om eenduidig te definiëren wat er met de informatie mag gebeuren. Wanneer informatie is voorzien van een TLP-aanduiding weet u met wie u deze informatie mag delen. Dit staat beschreven in de standaard First (www.first.org/tlp).

Ontvangers van TLP:WHITE mogen de informatie publiek verspreiden.

Uw reacties zijn welkom op info@ncsc.nl

Feiten

Zoom heeft kwetsbaarheden verholpen in Zoom Workplace en Zoom Clients (Specifiek voor versies vóór 6.5.10).

Duiding

De kwetsbaarheden omvatten onder andere ongepaste validatie van certificaten, cross-site scripting, en onjuiste behandeling van gevoelige informatie, wat kan leiden tot ongeautoriseerde toegang en informatie openbaarmaking door zowel geauthenticeerde als ongeauthenticeerde gebruikers.

Oplossingen

Zoom heeft updates uitgebracht om de kwetsbaarheden te verhelpen. Zie bijgevoegde referenties voor meer informatie.

Referenties

- <https://www.zoom.com/en/trust/security-bulletin/ZSB-25040/>
- <https://www.zoom.com/en/trust/security-bulletin/ZSB-25041/>
- <https://www.zoom.com/en/trust/security-bulletin/ZSB-25042/>
- <https://www.zoom.com/en/trust/security-bulletin/ZSB-25043/>
- <https://www.zoom.com/en/trust/security-bulletin/ZSB-25044/>
- <https://www.zoom.com/en/trust/security-bulletin/ZSB-25045/>
- <https://www.zoom.com/en/trust/security-bulletin/ZSB-25046/>
- <https://www.zoom.com/en/trust/security-bulletin/ZSB-25047/>
- <https://www.zoom.com/en/trust/security-bulletin/ZSB-25048/>

Kwetsbaarheden

CVE	CVSS Score
➤ CVE-2025-30662	4.8 MEDIUM
➤ CVE-2025-30669	6.3 MEDIUM
➤ CVE-2025-62482	5.3 MEDIUM
➤ CVE-2025-62483	6.9 MEDIUM
➤ CVE-2025-62484	5.3 MEDIUM

> CVE-2025-64738	4.8 MEDIUM
> CVE-2025-64739	5.3 MEDIUM
> CVE-2025-64740	7.3 HIGH
> CVE-2025-64741	4.8 MEDIUM

CWE's

CWE	Beschrijving
> CVE-61	UNIX Symbolic Link (Symlink) Following
> CVE-73	External Control of File Name or Path
> CVE-74	Improper Neutralization of Special Elements in Output Used by a Downstream Component ('Injection')
> CVE-79	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')
> CVE-200	Exposure of Sensitive Information to an Unauthorized Actor
> CVE-212	Improper Removal of Sensitive Information Before Storage or Transfer
> CVE-285	Improper Authorization
> CVE-295	Improper Certificate Validation
> CVE-347	Improper Verification of Cryptographic Signature
> CVE-646	Reliance on File Name or Extension of Externally-Supplied File
> CVE-1333	Inefficient Regular Expression Complexity

Getroffen producten

Zoom Communications Inc.
Zoom Workplace

Zoom Workplace Clients
Zoom Workplace VDI Client
Zoom Workplace VDI Plugin macOS Universal installer
Zoom Workplace for Android
Zoom Workplace for macOS

Disclaimer

The Netherlands Cyber Security Center (henceforth: NCSC-NL) maintains this page to enhance access to its information and security advisories. The use of this security advisory is subject to the following terms and conditions: NCSC-NL makes every reasonable effort to ensure that the content of this page is kept up to date, and that it is accurate and complete. Nevertheless, NCSC-NL cannot entirely rule out the possibility of errors, and therefore cannot give any warranty in respect of its completeness, accuracy or continuous keeping up-to-date. The information contained in this security advisory is intended solely for the purpose of providing general information to professional users. No rights can be derived from the information provided therein. NCSC-NL and the Kingdom of the Netherlands assume no legal liability or responsibility for any damage resulting from either the use or inability of use of this security advisory. This includes damage resulting from the inaccuracy of incompleteness of the information contained in the advisory. This security advisory is subject to Dutch law. All disputes related to or arising from the use of this advisory will be submitted to the competent court in The Hague. This choice of means also applies to the court in summary proceedings.