Nationaal Cyber Security Centrum
Ministerie van Justitie en Veiligheid

NCSC-2026-0249

Kwetsbaarheden verholpen in Zoom

NCSC Security Advisory
Prioriteit: Normaal
Gepubliceerd op: 17-07-2026

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 Client voor Windows, Zoom Rooms voor Windows en andere Zoom Windows-producten zoals de Windows Desktop Client, VDI Client en Meeting SDK.

Duiding

De kwetsbaarheden betreffen onder andere een TOCTOU race condition die door een geauthenticeerde lokale gebruiker kan worden misbruikt om privileges te escaleren. Daarnaast is er een onjuiste privilege management in Zoom Rooms voor Windows (versies eerder dan 7.1.0), waardoor geauthenticeerde lokale gebruikers hogere toegangsrechten kunnen verkrijgen dan bedoeld. Verder zijn er problemen met onjuiste inputvalidatie in de Zoom Windows Desktop Client, VDI Client en Meeting SDK, waardoor niet-geauthenticeerde aanvallers via netwerktoegang controle over gebruikersaccounts kunnen verkrijgen. Deze kwetsbaarheden ontstaan door onvoldoende validatie van inputdata en inadequate handhaving van privilege boundaries binnen de applicaties.

Oplossingen

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

Referenties

- https://www.zoom.com/en/trust/security-bulletin/ZSB-26011/
- https://www.zoom.com/en/trust/security-bulletin/ZSB-26012/
- https://www.zoom.com/en/trust/security-bulletin/ZSB-26013/
- https://www.zoom.com/en/trust/security-bulletin/ZSB-26014/

Kwetsbaarheden

CVE	CVSS Score
CVE-2026-53410	7.0 HIGH
CVE-2026-53409	7.8 HIGH
CVE-2026-53411	7.8 HIGH
CVE-2026-53412	9.8 CRITICAL

CWE's

CWE	Beschrijving
CWE-20	Improper Input Validation
CWE-367	Time-of-check Time-of-use (TOCTOU) Race Condition

Getroffen producten

Zoom Communications
Zoom Clients
Zoom Rooms
Zoom Workplace VDI Plugin
Zoom Workplace for Windows
Zoom Video Communications
Zoom Video Communications Rooms
Zoom Video Communications Workplace

Disclaimer