Nationaal Cyber Security Centrum
Ministerie van Justitie en Veiligheid

NCSC-2026-0223

Kwetsbaarheden verholpen in BeyondTrust Remote Support en Privileged Remote Access

NCSC Security Advisory
Prioriteit: Normaal
Gepubliceerd op: 10-07-2026

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

BeyondTrust heeft kwetsbaarheden verholpen in de producten Remote Support en Privileged Remote Access.

Duiding

De kwetsbaarheden betreffen meerdere aspecten van de producten Remote Support en Privileged Remote Access. Er is een pre-authenticatie kwetsbaarheid die een netwerkgebaseerde aanvaller in staat stelt om toegangcontroles te omzeilen zonder voorafgaande authenticatie, mits een specifieke authenticatieconfiguratie is ingeschakeld. Hierdoor kan een aanvaller ongeautoriseerde en mogelijk verhoogde toegang verkrijgen. Daarnaast is er een probleem met onvoldoende validatie van clientinput in het netwerkcommunicatiesubsyteem, waardoor een niet-geauthenticeerde aanvaller een denial-of-service kan veroorzaken door normale netwerkcommunicatie te verstoren. Verder kunnen geauthenticeerde gebruikers met beperkte rechten door onvoldoende inputvalidatie toegang krijgen tot niet-geautoriseerde bronnen, hoewel dit beperkt is tot accounts met specifieke permissies.

Oplossingen

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

Referenties

- https://www.beyondtrust.com/trust-center/security-advisories/bt26-03

Kwetsbaarheden

CVE	CVSS Score
CVE-2026-40140	8.7 HIGH
CVE-2026-40141	8.5 HIGH
CVE-2026-40138	9.2 CRITICAL
CVE-2026-40139	9.2 CRITICAL

CWE's

CWE	Beschrijving
CWE-287	Improper Authentication
CWE-400	Uncontrolled Resource Consumption
CWE-943	Improper Neutralization of Special Elements in Data Query Logic

Getroffen producten

BeyondTrust
Privilege Remote Access
Remote Support

Disclaimer