



Advisory NCSC-2026-0437

PRIORITEIT: HOOG

Kwetsbaarheid verholpen in BeyondTrust Remote Support

Publicatiedatum: 16-10-2026

Toegestane verspreiding: TLP:WHITE
(Traffic Light Protocol)

Deze publicatie bevat het label TLP:WHITE en wordt door het Nationaal Cyber Security Center (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.

Reacties zijn welkom op info@ncsc.nl.

Feiten

BeyondTrust heeft een kritieke kwetsbaarheid verholpen in BeyondTrust Remote Support.

Duiding

De kwetsbaarheid met kenmerk CVE-2026-102764 heeft een CVSS-score van 9.3 en betreft onvoldoende validatie van de herkomst van berichten binnen de interne componenten van het product. Hierdoor kan een niet-geauthenticeerde kwaadwillende de kwetsbaarheid op afstand misbruiken om bestanden op een getroffen appliance te plaatsen of te wijzigen. Alle Remote Support-versies tot en met 26.2.3 zijn getroffen. BeyondTrust bevestigt dat CVE-2026-102764 als zeroday-kwetsbaarheid is misbruikt.

Oplossingen

BeyondTrust heeft de BT26-05-RS patch uitgebracht voor Remote Support 24.3.1 tot en met 26.2.3 om de kwetsbaarheid te verhelpen. Oudere self-hosted versies moeten eerst worden bijgewerkt naar een ondersteunde versie. Het NCSC adviseert om de beveiligingsupdate met spoed toe te passen en kwetsbare systemen te onderzoeken op aanwijzingen voor eerdere compromittering. Zie bijgevoegde referenties voor meer informatie.

Referenties

- <https://www.beyondtrust.com/blog/entry/bt26-05>
- <https://www.beyondtrust.com/trust-center/security-advisories/bt26-05>

Kwetsbaarheden

CVE	CVSS Score
CVE-2026-102764	9.3 CRITICAL

CWE's

CWE	Beschrijving
CWE-290	Authentication Bypass by Spoofing

Getroffen producten

BeyondTrust
Remote Support

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 or 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.