contact@namiq.io · namiq.io

NamiQ

SECURITY ADVISORY

BeyondTrust Remote Support exploited

CVE-2026-102764 · on CISA's exploited list since 16 October 2026

Analysis Report

If you run BeyondTrust Remote Support on 26.2.3 or earlier, act today: CISA's 19 October 2026 date has already passed. First find out whether you run it and which version, because the record names no …

PREPARED BY	NamiQ	DATE	1 November 2026
FACTS AS OF	1 November 2026	VERSION	1.0
SEVERITY	**Critical: CVSS 4.0 9.3**	STATUS	On CISA's exploited list; due 19 October 2026

NamiQ © 2026 NamiQ. All rights reserved. This document is the property of NamiQ. It may be shared unaltered, with attribution.
Companion article: namiq.io/insights/beyondtrust-remote-support-cve-2026-102764

The bottom line

> *If you run BeyondTrust Remote Support on 26.2.3 or earlier, act today: CISA's 19 October 2026 date has already passed. First find out whether you run it and which version, because the record names no fixed version.*

At a glance

Fact	Detail
Product	BeyondTrust Remote Support (CVE-2026-102764)
Severity	Critical: 9.3 (CVSS 4.0)
CISA	On its exploited list since 16 October 2026. Deadline for US federal agencies: 19 October 2026.
Chance of exploitation (EPSS)	0.19, the estimated chance in the next 30 days, as at 1 November 2026
Ransomware use	Not recorded by CISA. That is not the same as none.
Fixed in	No source we read names a fixed version
Who looks first	Firms and IT providers that run a BeyondTrust Remote Support appliance on version 26.2.3 or earlier. The record names no other condition. If you do not run it, you can stop reading.

Does this apply to you?

Answer in order. Stop at the first no.

Question	If no	If yes
Do you or your IT provider run BeyondTrust Remote Support?	Nothing to do for this CVE.	Check the version (next question).
Is the version 26.2.3 or earlier?	Ask the vendor to confirm in writing that your version is unaffected.	You are in the affected range. Go to the next question.
Can anyone outside your own staff reach the appliance over a network?	Lower urgency, but still ask the vendor what to apply.	Treat it as exposed now and restrict access while you wait for a fix.

What it is

The record says internal components did not properly check where messages came from. An attacker could send spoofed messages and, under the right conditions, perform file operations on the appliance. CISA says the attacker can be remote.

Why it matters

Our reading is that an appliance which accepts spoofed messages and lets a stranger change files should be treated as exposed until shown otherwise. The record scores it 9.3 (CVSS 4.0) and lists CWE-290, authentication bypass by spoofing. It does not say whether a login is needed, so assume none until the vendor says otherwise.

Things people will get wrong

- "It only touches files, so it is minor." The record gives 9.3 and CISA lists it as exploited. The sources do not say how far file operations can go, so do not assume the damage is small.
- "We are patched because we are on the latest version we know of." The record names no fixed version. Only the affected range, up to and including 26.2.3, is stated.

How we would triage it

This is our judgement.

Step 1: Find the versions you run

- Ask your IT provider whether Remote Support is in use and where it is hosted.
- Read the version from the appliance's admin screen and compare it with 26.2.3.

Step 2: Reduce exposure

- Restrict who can reach the appliance to known networks while no fix is confirmed.
- Ask the vendor for its mitigation instructions, as CISA's required action points to them.

Step 3: Apply the vendor's fix

- Ask the vendor which version fixes this CVE, since no source here names one.
- Apply it and record the version and date.

Step 4: Check for signs of misuse

- Review the appliance for file changes you cannot explain, going back to before 15 October 2026.

To close it, read the version from the product itself, not from an old inventory, and save the output with the date. If you cannot update today, write down who owns it, the new date, and what limits exposure until then.

Send this to your IT provider

Copy it, change the names and dates, and send it. It is a draft for you to check, not a template tested with any provider.

> *Hello, we need to know whether we run BeyondTrust Remote Support, and if so where and which version. CVE-2026-102764 affects all versions up to and including 26.2.3, and CISA lists it as exploited with a due date of 19 October 2026. The record names no fixed version, so please tell us the vendor's fix and mitigations. Please also tell us whether the appliance can be reached from the internet, and confirm in writing the version we run and that the fix is applied, as soon as you can. Thank you.*

Signs it was used

An update closes the hole. It does not tell you whether someone used it first. CISA's required action points to its forensic triage requirements (BOD 26-04). Look for:

- File changes or new files on the appliance that nobody on your team made.
- Connections to the appliance from addresses you do not recognise.
- Anything unexpected on the appliance from 15 October 2026 onward.

The weakness behind it

The record classes this as CWE-290 (Authentication Bypass by Spoofing).

The sources, in their words

CISA's catalogue entry:

> *BeyondTrust Remote Support contains an authentication bypass by spoofing vulnerability that could allow a remote attacker to perform file operations on the appliance.*

The CVE record, published by BT on 15 October 2026:

> *The vulnerability exists within internal components of BeyondTrust's Remote Support product. The components did not adequately validate the origin of the messages it received. Under the right conditions, this could allow an attacker to perform file operations on the appliance.*

Versions of BeyondTrust Remote Support the record lists as affected:

- all versions up to and including 26.2.3

CISA's required action:

> *Apply mitigations in accordance with vendor instructions, ensuring compliance with CISA's BOD 26-04 Prioritizing Security Updates Based on Risk (see URL in Notes) guidance and CISA's "Forensics Triage Requirements" (see URL in Notes).*

What we do not know yet

- Which version fixes this flaw: no source here names one.
- Whether an attacker needs a login or any prior access.
- What the record means by "the right conditions".
- How far file operations on the appliance can be taken.
- We have not tested this against any environment. Versions and scores are as the sources state them and as at 1 November 2026; the vendor's advisory wins where it differs.
- The sections headed "The bottom line", "Does this apply to you?", "What it is", "Why it matters", "Exposure by situation", "Things people will get wrong", "How we would triage it" and "Send this to your IT provider" are our interpretation of the sources, not a statement by CISA or the vendor.

Appendix 1. Severity decoded

CVE-2026-102764: score 9.3, `CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:N/VC:H/VI:H/VA:H/SC:N/SI:N/SA:N` As the CVE record gives it. The record's own score can differ from the base score on the NVD record.

Metric	Value	What it means here
Attack vector	Network	Reachable over a network, with no need to be on the same segment.
Attack complexity	Low	No special conditions beyond the flaw itself.
Attack requirements	None	Works against a default deployment.
Privileges required	None	No account is needed.
User interaction	None	No one has to do anything.
Vulnerable system: confidentiality	High	Total loss of confidentiality.
Vulnerable system: integrity	High	Total loss of integrity.
Vulnerable system: availability	High	Total loss of availability.
Subsequent systems: confidentiality	None	No data exposed.
Subsequent systems: integrity	None	Nothing can be altered.
Subsequent systems: availability	None	No effect on availability.

Appendix 2. Timeline

Date	Event
15 October 2026	CVE record published by BT.
16 October 2026	CISA added it to its list of exploited vulnerabilities.
19 October 2026	CISA's deadline for US federal agencies.

Appendix 3. Exposure by situation

These priorities are our judgement from the attacker prerequisites in the sources. They are not vendor ratings.

Your situation	Priority	Timeframe

Affected version, and the appliance can be reached from the internet	High	Today
Affected version, reachable only from your internal network	High	Within days; CISA's date has passed
Version not yet checked	High	Today: find the version first
Version above 26.2.3, confirmed by the vendor	Low	Ask for written confirmation
You do not run Remote Support	None	None for this CVE

Appendix 4. Definition of done

- Every BeyondTrust Remote Support you run is listed, with its version.
- Each is outside the affected list, or the vendor's mitigation is in place.
- The version output or a screenshot is saved with the date.
- Logs for the weeks before the update were searched, and anything odd was written down.
- Anything not done has an owner and a date.

Sources

- CISA Known Exploited Vulnerabilities catalogue: https://www.cisa.gov/known-exploited-vulnerabilities-catalog
- CVE record for CVE-2026-102764: https://www.cve.org/CVERecord?id=CVE-2026-102764
- FIRST: Exploit Prediction Scoring System: https://www.first.org/epss/
- Reference in the CVE record: nvd.nist.gov: https://nvd.nist.gov/vuln/detail/CVE-2026-102764
- Reference in the CVE record: www.beyondtrust.com: https://www.beyondtrust.com/blog/entry/bt26-05
- Reference in the CVE record: beyondtrustcorp.service-now.com: https://beyondtrustcorp.service-now.com/csm?id=csm_kb_article&sysparm_article=KB0024066