GOVERNMENT OF THE REPUBLIC OF VANUATU

PRIME MINISTER'S OFFICE

CERTVU
DEPARTMENT OF COMMUNICATIONS & DIGITAL TRANSFORMATION

PM B 9108 Port Vila, Vanuatu

Tel: (678) 33380

GOUVERNEMENT DE LA REPUBLIQUE DU VANUATU

BUREAU DU PREMIER MINISTRE

CERTVU

DEPARTMENT DE COMMUNICATION ET DE TRANSFORMATION NUMERIQUE

SPP 9108 Port Vila, Vanuatu
Tel: (678) 33380

21 October 2026

Advisory 360: BeyondTrust Remote Support Authentication Bypass Leading to Arbitrary File Upload Vulnerability - Actively Exploited Zero-Day (CVE-2026-102764).

Release Date: 16th October 2026
Impact: CRITICAL
TLP: CLEAR

The Department of Communications and Digital Transformation (DCDT) through CERT Vanuatu (CERTVU), provides the following advisory.

This alert is relevant to Organizations and System/Network administrators that utilize the above product(s). This alert is intended to be understood by technical users and systems administrators.

What is it?

CVE-2026-102764 is an authentication bypass by spoofing (CWE-290) in BeyondTrust Remote Support. Internal messaging components did not adequately validate the origin of the messages they received, so a remote, unauthenticated attacker can perform file operations on the appliance, including uploading arbitrary files, without credentials or user interaction. BeyondTrust rates it CVSS v4.0 9.3 (Critical), and NVD analysis was still pending at the time of writing. BeyondTrust published advisory BT26-05 on 15 October 2026. The issue is a zero-day and was exploited before a patch was available.

What are the systems affected?

The following self-managed products are affected:

- BeyondTrust Remote Support, all versions up to and including 26.2.3
- BeyondTrust Privileged Remote Access (self-hosted): shares the affected code. No exploitation path has been found, but BeyondTrust recommends a precautionary patch

Not affected / patched version:

- Patch BT26-05-RS for Remote Support versions 24.3.1 to 26.2.3. Versions older than 24.3.1 must first be upgraded to a supported release, then patched
- Remote Support SaaS customers were patched automatically by BeyondTrust (8 or 9 October 2026, depending on the source) and need no action
- Self-hosted customers without automatic updates must apply the patch manually through the /appliance interface

What does this mean?

Successful exploitation may allow attackers to:

- Bypass authentication and upload arbitrary files, including web shells, to the appliance without credentials
- Gain root access to the appliance, steal administrator, API, SAML and vault credentials, and wipe logs
- Use the compromised remote support appliance, which holds privileged access to many internal systems, as a foothold for lateral movement across the network

Mitigation process

CERTVU recommends the following:

1. Patch immediately
Identify every Remote Support and Privileged Remote Access deployment, confirm whether it is SaaS or self-hosted, and verify the installed version. Apply patch BT26-05-RS to self-hosted appliances, upgrading versions older than 24.3.1 first. Confirm that automatic updates are enabled.

2. Restrict access to the appliance
Limit /login and /appliance to trusted networks and remove internet exposure where possible. This reduces the risk but does not replace patching.

3. Hunt for compromise
4. Preserve evidence and rebuild
5. Rotate credentials

Report suspected compromise to CERTVU.

Reference

1. https://www.beyondtrust.com/trust-center/security-advisories/bt26-05
2. https://beyondtrust.com/blog/entry/bt26-05
3. https://www.cisa.gov/known-exploited-vulnerabilities-catalog
4. https://cyber.gc.ca/en/alerts-advisories/al26-025-critical-vulnerability-impacting-beyondtrust-remote-support-cve-2026-102764
5. https://socradar.io/blog/cve-2026-102764-beyondtrust-zero-day/
6. https://www.bleepingcomputer.com/news/security/beyondtrust-patches-zero-day-exploited-in-attacks-since-august/
7. https://nvd.nist.gov/vuln/detail/CVE-2026-102764