Cal OES
GOVERNOR'S OFFICE
OF EMERGENCY SERVICES

Zero-Day Authentication Bypass Vulnerability in BeyondTrust Remote Support

Unauthenticated Remote Attacker | Arbitrary File Upload | Zero-Day Exploitation | Patch Available

The Cal-CSIC has become aware of an authentication bypass vulnerability (CVE-2026-102764) in BeyondTrust Remote Support. Remote Support versions 26.2.3 and earlier are affected when the BT26-05-RS patch has not been applied. The vulnerability carries a CVSS 4.0 score of 9.3.[1,2]

In unpatched versions of BeyondTrust's Remote Support, internal messaging components do not adequately validate the origin of received messages. A remote, unauthenticated attacker can use the flaw to perform file operations on a reachable appliance. Successful exploitation allows the attacker to upload arbitrary files to the appliance. Open-source reporting on a verified exploitation describes a web shell, subsequent escalation to root, and persistence established through separate post-exploitation steps.[1,2]

BeyondTrust released the BT26-05-RS patch for Remote Support versions 24.3.1 through 26.2.3; older installations must upgrade before applying it. All Remote Support software as service (SaaS) instances were patched by 9 October 2026. BeyondTrust also released a precautionary patch for self-hosted Privileged Remote Access because it shares code with the affected software, although vendor testing found no exploit path in that product. The vendor confirmed exploitation on 29 August 2026 against one hosted and one self-hosted Remote Support instance. The vulnerability was added to the Known Exploited Vulnerabilities catalog on 16 October. BeyondTrust has not reported technical exploit details, and no public proof of concept (PoC) has been observed as of 16 October 2026.[1,3,4]

The Cal-CSIC recommends that clients running self-hosted Remote Support immediately verify patch status and apply BT26-05-RS, upgrading first if their version is older than 24.3.1. Clients running self-hosted Privileged Remote Access should apply BeyondTrust's precautionary patch. Review off-appliance logs, privileged sessions, and unauthorized account or permission changes for appliances exposed since late-August 2026; preserve forensic evidence before rebuilding a suspected compromised appliance. If compromise is suspected, follow the vendor's incident guidance, as patching alone does not remove established access. Rotate stored or brokered credentials after the appliance has been secured.[1,2,3]

WARNING: This document is the property of the California Cybersecurity Integration Center (CAL-CSIC) and follows Traffic Light Protocol (TLP) standards. Except for **TLP: CLEAR**, all TLP designations require recipients to control, store, handle, transmit, and dispose of this product accordingly. Do not release to the public, media, or unauthorized personnel without prior CAL-CSIC approval. This document may contain information exempt from public release under the California Public Records Act (Govt. Code Sec. 7920.000 et seq.). CAL-CSIC does not guarantee the completeness or accuracy of the information.

For additional details regarding CVE-2026-102764, please use this link:

BeyondTrust Security Advisory:

https://www.beyondtrust.com/trust-center/security-advisories/bt26-05

Affected versions are unpatched installations. Versions older than v24.3.1 must be upgraded before BT26-05-RS can be applied.[1]

Affected Products and Versions

Product	Affected Version	Fixed Release
BeyondTrust Remote Support	All versions through 26.2.3	BT26-05-RS patch for v24.3.1-v26.2.3

Sharing, Reporting, and Support

Sharing, Reporting, and Support

Sharing information and intelligence to state, local, federal, and private partners will ensure organizations across California can be better informed and defended.

For questions, concerns, or support or are interested in sharing information or intelligence in any cyber related matter, contact the Cal-CSIC via:

833-REPORT-1 or 916.636.2997

calcsic@caloes.ca.gov

Report suspicious or suspected foreign activity and incidents to:

Federal Officials at CISA and/or the FBI as applicable

Coordinate with your regional Fusion Center

SHARE information, intelligence, and IOCs with ISACs

References

[1] BeyondTrust; "BT26-05"; https://www.beyondtrust.com/trust-center/security-advisories/bt26-05; accessed 16 October 2026

[2] Google Threat Intelligence Group and Mandiant; "ARMORY CASTLE Exploits BeyondTrust"; https://cloud.google.com/blog/topics/threat-intelligence/armory-castle-exploits-beyondtrust/; accessed 16 October 2026

[3] BeyondTrust Security Team; "ARMORY CASTLE and BT26-05: What Security Teams Need to Know"; https://www.beyondtrust.com/blog/entry/bt26-05; accessed 16 October 2026

[4] Cybersecurity and Infrastructure Security Agency; "Known Exploited Vulnerabilities Catalog"; https://www.cisa.gov/known-exploited-vulnerabilities-catalog; accessed 16 October 2026

WARNING: This document is the property of the California Cybersecurity Integration Center (CAL-CSIC) and follows Traffic Light Protocol (TLP) standards. Except for **TLP: CLEAR**, all TLP designations require recipients to control, store, handle, transmit, and dispose of this product accordingly. Do not release to the public, media, or unauthorized personnel without prior CAL-CSIC approval. This document may contain information exempt from public release under the California Public Records Act (Govt. Code Sec. 7920.000 et seq.). CAL-CSIC does not guarantee the completeness or accuracy of the information.