

CVE-2026-1731

BeyondTrust Remote Support (RS) and Privileged Remote Access (PRA) OS Command Injection Vulnerability

Exigent CISA KEV since Feb 13, 2026 Actively exploited Ransomware use known Public exploit module (Metasploit)

BeyondTrust Remote Support (RS) and certain older versions of Privileged Remote Access (PRA) contain a critical pre-authentication remote code execution vulnerability. By sending specially crafted requests, an unauthenticated remote attacker may be able to execute operating system commands in the context of the site user.

EVRS 95 / ₁₀₀ Immediate priority	CVSS V4.0 9.9 Critical · NVD	EPSS 0.925 99.83rd percentile · FIRST	CISA DEADLINE Feb 16, 2026 CISA federal deadline · Overdue by 8 months
--	--	---	--

Signals behind the score

☒ counted in the score ☐ not counted evidence for 6 of 8 signals

☒ CISA KEV	Listed in the catalog	☐ Vendor exploitation	Confirmed exploitation in the wild
☒ Ransomware	Known ransomware campaigns	☐ KEV recency	Added to CISA KEV within the last year
☒ EPSS	0.925 probability	☐ Pre-patch disclosure	Disclosure status unavailable
☒ CVSS	Base score 9.9	☐ Microsoft Exploitability Index	Not a Microsoft CVE

Remediation

Out-of-band / urgent Patch or fixed version identified

CISA required action: Apply mitigations per vendor instructions, follow applicable BOD 22-01 guidance for cloud services, or discontinue use of the product if mitigations are unavailable. **CISA note:** Please adhere to the vendor's guidelines to assess exposure and mitigate risks. Check for signs of potential compromise on all internet accessible BeyondTrust products affected by this vulnerability. For more information please see: <https://www.beyondtrust.com/trust-center/security-advisories/bt26-02>
Basis: CISA KEV required action

Affected and fixed versions

PACKAGE	AFFECTED	FIXED IN	SOURCE
privileged remote access	< 25.1	25.1	NVD
remote support	< 25.3.2	25.3.2	NVD

Sources

Vendor guidance	github.com/advisories/GHSA-p5wr-5p37-2wm6	Additional guidance	beyondtrust.com/trust-center/security-advisories/bt26-02
NVD	nvd.nist.gov/vuln/detail/CVE-2026-1731	CISA KEV	cisa.gov/known-exploited-vulnerabilities-catalog
ENISA EUVD	euvd.enisa.europa.eu/vulnerability/EUVD-2026-5559	Current data	evulnable.com/vulnerability-management/cve/CVE-2026-1731

Snapshot at generation time. EPSS can move quickly. A public exploit module is not evidence of active exploitation.