

CVE-2024-12356

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

CISA KEV since Dec 19, 2024

Actively exploited

Public exploit module (Metasploit)

A critical vulnerability has been discovered in Privileged Remote Access (PRA) and Remote Support (RS) products which can allow an unauthenticated attacker to inject commands that are run as a site user.

EVRS 85/100 Immediate priority	CVSS V3.1 9.8 Critical · NVD	EPSS 0.873 99.75th percentile · FIRST	CISA DEADLINE Dec 27, 2024 KEV since 2024 · listed over a year
--	--	---	--

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	No known ransomware campaign association	☐ KEV recency	Added to CISA KEV within the last two years
☒ EPSS	0.873 probability	☐ Pre-patch disclosure	Disclosure status unavailable
☒ CVSS	Base score 9.8	☐ Microsoft Exploitability Index	Not a Microsoft CVE

Remediation

Patch Immediately Patch or fixed version identified

CISA required action: Apply mitigations per vendor instructions or discontinue use of the product if mitigations are unavailable.
Basis: CISA KEV required action

Affected and fixed versions

PACKAGE	AFFECTED	FIXED IN	SOURCE
privileged remote access	≤ 24.3.1	after 24.3.1	NVD
remote support	≤ 24.3.1	after 24.3.1	NVD

Sources

Vendor guidance github.com/advisories/GHSA-69c6-ccv7-v3g3

Additional guidance beyondtrust.com/trust-center/security-advisories/bt24-10

NVD nvd.nist.gov/vuln/detail/CVE-2024-12356

CISA KEV cisa.gov/known-exploited-vulnerabilities-catalog

ENISA EUVD euvd.enisa.europa.eu/vulnerability/EUVD-2024-50801

Current data evulnable.com/vulnerability-management/cve/CVE-2024-12356

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