An Lárionad Náisiúnta Cibearshlándála
National Cyber Security Centre

NCSC #2412180143

NCSC Advisory

Critical Vulnerability found in BeyondTrust Remote Support & Privileged Remote Access

CVE-2024-12356
(CVSS: 9.8)

18th, December 2024

STATUS: TLP:CLEAR

Recipients can spread this to the world, there is no limit on disclosure. Sources may use **TLP:CLEAR** when information carries minimal or no foreseeable risk of misuse, in accordance with applicable rules and procedures for public release. Subject to standard copyright rules, TLP:CLEAR information may be shared without restriction.

For more information on the Traffic Light Protocol, see https://www.first.org/tlp/. Please treat this document in accordance with the TLP assigned.

An Roinn Comhshaoil, Aeráide agus Cumarsáide
Department of the Environment, Climate and Communications

Description

CVE ID: CVE-2024-12356

Published: 2024-12-17

Vendor: BeyondTrust

Products: Remote Support & Privileged Remote Access

CVSS Score[1]: 9.8

Products affected

Product	Version
Remote Support & Privileged Remote Access	24.3.1 and earlier

Impact

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.

List of Known Indicators of Compromise (IoC):

IPv4 Addresses	IPv6 Addresses
24.144.114.85	2604:a880:400:d1::7293:c001
142.93.119.175	2604:a880:400:d1::72ad:3001
157.230.183.1	2604:a880:400:d1::7716:1
192.81.209.168	2604:a880:400:d1::7df0:7001
	2604:a880:400:d1::8622:f001

[1] https://www.first.org/cvss/v3.0/specification-document

Common Weakness Enumeration (CWE)[2]: CWE-77 Improper Neutralization of Special Elements used in a Command ('Command Injection')

Known Exploited Vulnerability (KEV) catalog[3]: No

Used by Ransomware Operators: N/A

Recommendations

The NCSC strongly recommends installing updates for vulnerable systems with the highest priority, after thorough testing. Affected organisations should review the latest release notes and install the relevant updates from BeyondTrust.

- https://nvd.nist.gov/vuln/detail/CVE-2024-12356
- https://www.cve.org/CVERecord?id=CVE-2024-12356
- https://www.beyondtrust.com/trust-center/security-advisories/bt24-10
- https://www.beyondtrust.com/remote-support-saas-service-security-investigation

[2] https://cwe.mitre.org

[3] https://www.cisa.gov/known-exploited-vulnerabilities-catalog