# Bitwarden Server < 2026.4.0 Missing Authorization via Provider Clients

MITRE | NVD | CVE.ORG | JSON API | Print: PDF

## Summary

| | |
|---|---|
| **CVE** | CVE-2026-43639 |
| **State** | PUBLISHED |
| **Assigner** | VulnCheck |
| **Source Priority** | CVE Program / NVD first with legacy fallback |
| **Published** | 2026-05-11 18:16:36 UTC |
| **Updated** | 2026-05-11 18:16:36 UTC |
| **Description** | Bitwarden Server prior to v2026.4.0 contains a missing authorization vulnerability that allows a provider service user to add |

## Risk And Classification

**Primary CVSS:** v4.0 8.9 HIGH from disclosure@vulncheck.com

CVSS:4.0/AV:N/AC:H/AT:N/PR:H/UI:N/VC:H/VI:H/VA:H/SC:H/SI:H/SA:H/E:X/CR:X/IR:X/AR:X/MAV:X/MAC:X/MAT:X/MPR:X/MUI:X/MVC:X/MVI:X/MVA:X/MSC:X/MSI:X/MSA:X/S:X/AU:X/R:X/V:X/RE:X/U:X

**Problem Types:** CWE-862 | CWE-862 Missing Authorization

| Version | Source | Type | Score | Severity | Vector |
|---|---|---|---|---|---|
| 4.0 | disclosure@vulncheck.com | Secondary | 8.9 | HIGH | CVSS:4.0/AV:N/AC:H/AT:N/PR:H/UI:N/VC:H/VI:H/VA:H/SC:H/SI:H/SA |
| 4.0 | CNA | CVSS | 8.9 | HIGH | CVSS:4.0/AV:N/AC:H/AT:N/PR:H/UI:N/VC:H/VI:H/VA:H/SC:H/SI:H/SA |
| 3.1 | disclosure@vulncheck.com | Primary | 8 | HIGH | CVSS:3.1/AV:N/AC:H/PR:H/UI:N/S:C/C:H/I:H/A:H |
| 3.1 | CNA | CVSS | 8 | HIGH | CVSS:3.1/AV:N/AC:H/PR:H/UI:N/S:C/C:H/I:H/A:H |

## CVSS v4.0 Breakdown

Attack Vector

Network

Attack Complexity

High

Attack Requirements

None

Privileges Required

High

User Interaction

None

None

Confidentiality

High

Integrity

High

Availability

High

Sub Conf.

High

Sub Integrity

High

Sub Availability

High

CVSS:4.0/AV:N/AC:H/AT:N/PR:H/UI:N/VC:H/VI:H/VA:H/SC:H/SI:H/SA:H/E:X/CR:X/IR:X/AR:X/MAV:X/MAC:X/MAT:X/MPR:X/MUI:X/MVC:X/MVI:X/MVA:X/MSC:X/MSI:X/MSA:X/S:X/AU:X/R:X/V:X/RE:X/U:X

## CVSS v3.1 Breakdown

Attack Vector

Network

Attack Complexity

High

Privileges Required

High

User Interaction

None

Scope

Changed

Confidentiality

High

Integrity

High

Availability

High

CVSS:3.1/AV:N/AC:H/PR:H/UI:N/S:C/C:H/I:H/A:H

## Vendor Declared Affected Products

| Source | Vendor | Product | Version | Platforms |
|---|---|---|---|---|
| CNA | Bitwarden | Server | affected 2026.4.0 semver | Not specified |

## References

| Reference | Source | Link | T |
|---|---|---|---|
| www.vulncheck.com/advisories/bitwarden-server-missing-authorization-via-provide... | disclosure@vulncheck.com | www.vulncheck.com | |

| | | |
|---|---|---|
| sanjokkarki.com.np/blog/bitwarden-provider-takeover | disclosure@vulncheck.com | sanjokkarki.com.np |
| github.com/bitwarden/server/commit/0918bfdda6f5eec391c69bd9074f6aef4eac0b1d | disclosure@vulncheck.com | github.com |
| github.com/bitwarden/server/releases/tag/v2026.4.0 | disclosure@vulncheck.com | github.com |
| github.com/bitwarden/server/pull/7372 | disclosure@vulncheck.com | github.com |
| CVE Program record | CVE.ORG | www.cve.org c |
| NVD vulnerability detail | NVD | nvd.nist.gov c |

## Vendor Comments And Credit

Discovery Credit

**CNA:** Sanjok Karki (en)

There are currently no legacy QID mappings associated with this CVE.