HCSEC-2025-33 - Vault Terraform Provider Applied Incorrect Defaults for LDAP Auth Method

security-vault, security-terraform

---

mickael 1 November 21, 2025, 2:23pm

Bulletin ID: HCSEC-2025-33
Affected Products / Versions: Vault Terraform Provider from v4.2.0 up to v5.4.0, fixed in v5.5.0.

Publication Date: November 21, 2025

Summary
Vault's Terraform Provider incorrectly set the default deny_null_bind parameter for the LDAP auth method to false by default, potentially resulting in an insecure configuration. If the underlying LDAP server allowed anonymous or unauthenticated binds, this could result in authentication bypass. This vulnerability, CVE-2025-13357, is fixed in Vault Terraform Provider v5.5.0.

Background
The **Vault Terraform Provider** uses Vault's API and allows users to administer Vault using a configuration file. Vault's **LDAP auth method** allows users to authenticate to Vault using an LDAP server. The LDAP auth method's **deny_null_bind** parameter was used by Vault to explicitly allow unauthenticated binds, if permitted by the LDAP server.

Details
If a Vault LDAP auth backend was created with the Vault Terraform Provider versions v4.2.0 to v5.4.0, the value of deny_null_bind parameter defaulted to false if the parameter was not specified in the Terraform file. Starting with Vault Terraform Provider v5.5.0, the provider will now correctly set this parameter to true by default. Vault 1.21.1, 1.20.6, 1.19.12, and 1.16.28 will also no longer accept empty password strings, preventing unauthenticated or anonymous binds to the LDAP server though the LDAP auth method. This deprecated parameter will be removed in a future version of Vault.

Remediation
Customers should evaluate the risk associated with this issue and ensure deny_null_bind is set to true in their LDAP auth method configuration. Customers should also consider upgrading to Vault Community Edition 1.21.1 and Vault Enterprise 1.21.1, 1.20.6, 1.19.12, and 1.16.28, which no longer allows Vault to perform unauthenticated or null binds against the LDAP server.

Otherwise, customers can upgrade the Vault Terraform Provider to v5.5.0, or explicitly set the deny_null_bind parameter to true in the Terraform files for any version of the Vault Terraform provider, and apply the changes.

Acknowledgement

This issue was identified by a third party who reported it to HashiCorp.

We deeply appreciate any effort to coordinate disclosure of security vulnerabilities. For information about security at HashiCorp and the reporting of security vulnerabilities, please see ***https://hashicorp.com/security****.*

Related topics

Topic	Replies	Activity
HCSEC-2023-24 - Vault's LDAP Auth Method Allows for User Enumeration security-vault	0	July 31, 2023
Issue with Vault provider in 0.12 vault	2	January 14, 2021
HCSEC-2020-25 - Vault’s LDAP Auth Method Allows User Enumeration security-vault	0	December 16, 2020
HCSEC-2021-11 - Terraform’s Vault Provider Did Not Correctly Configure Bound Labels for GCP Auth security-vault, security-terraform	0	April 21, 2021
Error: feature not enabled on current Vault version. min version required=1.15.0	2	August 15, 2024