HashiCorp

Terraform Enterprise's Management Console May Expose Sensitive Data

Vulnerability ID: CVE-2020-10590
Embargoed Notification Date: April 27, 2020
Release Date: May 11, 2020
Affected Products/Versions: Previous versions of Terraform Enterprise; fixed in v202002-2.
Rating: Critical

This security bulletin is provided to HashiCorp's Terraform Enterprise customers under embargo, and should be considered private until the release date noted above. All Terraform Enterprise customers are recommended to review the bulletin and take immediate remediation actions as documented.

A vulnerability was identified in Terraform Enterprise's third-party solution for on-premise application deployment, Replicated, such that an unauthenticated management API endpoint may expose sensitive data. This vulnerability affects all previous releases of Terraform Enterprise, and was fixed in the v202002-2 release.

This document outlines details about this vulnerability and describes steps for remediation.

Background

Terraform Enterprise utilizes Replicated, a third-party solution for on-premise application deployment, to facilitate the packaging, installation, operation, and update of Terraform Enterprise.

Vulnerability Details

During an internal security review, HashiCorp identified a vulnerability that permitted access to sensitive data via an unauthenticated API endpoint associated with the Replicated Management Console.

When a Terraform Enterprise server is connected to a network and port 8800 is accessible, this Replicated API endpoint may be accessed. This unauthenticated API may expose sensitive information, with the extent determined by the configuration of the Management Console and associated infrastructure. Depending on the configuration of a customer's Terraform Enterprise installation, this vulnerability could lead to the exposure of the TLS private key configured in the management console.

This vulnerability was reported to Replicated for triage and remediation. Terraform Enterprise was migrated to Replicated 2.42.5, which contains a fix for the vulnerability, in release v202002-2 (released on March 18).

Remediation

Terraform Enterprise may be deployed in "Online" or "Airgap" mode, and remediation steps differ according to mode:

- Customers running Terraform Enterprise in "Online" mode should urgently update their installations to Terraform Enterprise v202002-2 or newer. Replicated will be updated as part of this process. Please refer to Upgrading Terraform Enterprise for general guidance and version-specific upgrade notes.

- Customers running Terraform Enterprise in "Airgap" mode should urgently update the Replicated component independently. Please refer to Upgrading Replicated for guidance.

Alternatively, customers may consider triggering a Replicated upgrade without adopting a new Terraform Enterprise version. Steps to do so, for both "Online" and "Airgap" models, are documented in Upgrading Replicated.

After upgrading, customers can verify the current Replicated version by connecting to a Terraform Enterprise server and executing `replicated -version`. This should return 2.42.5 or newer.

Additional Considerations

Depending on the configuration of a customer's Terraform Enterprise installation, this vulnerability could lead to the exposure of the TLS private key configured in the management console.

If a customer has configured Terraform Enterprise with a custom TLS/SSL certificate, particularly a wildcard certificate, they should strongly consider revoking and replacing that certificate and associated private key. Steps for doing so within Terraform Enterprise are documented in How To Replace the TLS Certificate and Private Key.

Please contact support@hashicorp.com with any questions or security@hashicorp.com to report any security vulnerability or issue.