Dremio Vulnerability Management Policy

Dremio Vulnerability Management Policy

Date of Change	Responsible	Summary Of Change
June 2021	@ Emre Saglam	Initial Draft
July 2021	@ Emre Saglam	Vulnerability Management flow added

Purpose

This document covers Dremio's risk based approach to handle vulnerabilities and attaches SLAs to them

Scope

The scope of this document covers all the products that we create and put in front of our customers as well as all production internal Dremio systems. It also includes third party systems and libraries that Dremio depends on.

Ownership

The vulnerability scanning process is owned and operated by the security team. Engineering is responsible for timely delivery of patches following the Dremio Vulnerability Priority Definitions and SLAs.

Vulnerability Scanning

Scanning is done in a cadence that follows our Vulnerability Management Policy. Scanning must cover OS level patches, Application Security Vulnerabilities, Credential exposures and Third Party library dependencies.

Internal systems

Internal systems are scanned weekly using industry standard tools that can create metrics and reports for Dremio to measure the success of the rollout.

Products

Products that we put in front of our customers are scanned continuously using industry standard tools that can create metrics and reports for Dremio to measure the success of the rollout.

Remediation

All the vulnerabilities must be classified with a priority as defined in Dremio Vulnerability Priority Definitions and SLAs. These vulnerabilities must be fixed on time defined by the SLAs in the same document.

Definition of a Remediated Vulnerability

A vulnerability can be considered remediated if all of the conditions below are met:

1. When there is no known way to exploit the vulnerability after the remediation.
2. When every impacted resource has been covered with the remediation.
3. When the remediation is pushed into the production systems.
4. For a P0 vulnerability: when the remediation is tested by the Security team after the push to the production.

SLA Extensions

Any vulnerability that cannot be fixed on time will need an SLA extension with a mitigation and an action plan clearly defined in the extension request.

See Also

[Dremio Vulnerability Priority Definitions and SLAs]