VOSS

Insights Security Testing Process

October 19, 2022

Legal Information

Please take careful note of the following legal notices:

-
- This information is confidential. If received in error, it must be returned to VisionOSS ("VOSS"). Copyright in all documents originated by VOSS rests in VOSS. No portion may be reproduced by any process without prior written permission. VOSS does not guarantee that this document is technically correct or complete. VOSS accepts no liability for any loss (however caused) sustained as a result of any error or omission in the document.

Introduction

This document outlines the security practices that are used by VOSS as part of the software development lifecycle. A summary of the current vulnerability scan reports is also provided.

Process Overview

Change Management

GitLab is used as a source code management (SCM) tool. Code reviews are required before any software changes are merged into the mainline branch that is used for customer releases. A clear audit history is maintained for all changes and it is possible to revert any changes that introduce vulnerabilities or instability.

Security Testing

The Tenable Exposure Platform (Tenable.ep) is used for web application and vulnerability scanning.

Tenable.io Web Application Scanning

Dynamic web application security (DAST) scans are performed weekly using Tenable.io Web Application Scanning. These scans give insight into portal application vulnerabilities, including OWASP Top 10 exposures. Remediation suggestions are provided together with detailed information about any exposures detected.

Vulnerability Scanning

Tenable vulnerability management scans are performed weekly in order to give insight into host-specific vulnerabilities, including vulnerable operating system packages and port configurations. Remediation suggestions are provided together with detailed information about any exposures detected.

Incident Response

When high severity vulnerabilities are reported. VOSS performs internal risk assessment and publishes advisories with recommendations for remediation. Where necessary, patches will be made available for affected software releases.

Current Scan Results (as of 2022-09-26)

Insights Arbitrator Web Scan

An executive summary of the platform scan results show the following vulnerability findings:

Critical	High	Medium	Low	Info
0	0	23	1	89

The following must be noted:

- The Medium severity findings are due to the use of self-signed HTTPS. These findings do not affect production deployments, where trusted CA-signed certificates exist.
- The Low severity findings are due to the default SSH configuration. The customer may adjust this as needed in production deployments. The different settings are necessary depending on customer requirements.
- The Info severity findings include informational details regarding the scan.

Insights Dashboard Web Application Scan

An executive summary of the platform scan results show the following vulnerability findings:

Critical	High	Medium	Low	Info
0	0	28	0	143

The following must be noted:

- The Medium severity findings are due to the use of self-signed HTTPS. These findings do not affect production deployments, where trusted CA-signed certificates exist.
- The Info severity findings include informational details regarding the scan.

Insights DS9 Web Application Scan

An executive summary of the platform scan results show the following vulnerability findings:

Critical	High	Medium	Low	Info
0	0	8	0	76

The following must be noted:

- The Medium severity findings are due to the use of self-signed HTTPS. These findings do not affect production deployments, where trusted CA-signed certificates exist.
- The Info severity findings include informational details regarding the scan.