SKYBOX SECURITY

SKYBOX SECURITY, INC

Software Vulnerability Publishing Policy

Software Vulnerability Detection and Publishing Processes.

Skybox Security, Inc. | 2077 Gateway Place, Suite 200, San Jose, California 95110 USA | +1 866 675 9269

Overview

Purpose

The purpose of this document is to describe:

- The policy, process, and measures that Skybox Security takes to verify that our products are not exposed to vulnerabilities
- The response, remediation, and publishing processes if a vulnerability is found

Key Stakeholders

Name	Title	Email
Ami Ben Dror	CISO	ami@skyboxsecurity.com
Ron Davidson	VP R&D and CTO	ron.davidson@skyboxsecurity.com

Vulnerability Detection

Skybox employs a rigorous testing and quality assurance process before releasing our software to customers. Once released, Skybox takes several steps to detect potential vulnerabilities in the Skybox® Security Suite ("Application") and the Skybox Appliance family.

The processes described in this document apply to the Skybox Application, Skybox Appliance Web Admin and Skybox Appliance Linux packages.

Vulnerability Scan

Current Skybox Application and Appliance products are scanned every week to identify third-party library vulnerabilities that have been published and are present on the platform since the last scan.

Penetration Testing

Skybox conducts penetration testing for both Skybox Application and Skybox Appliance to identify new vulnerabilities.

Penetration testing is completed semiannually by a third-party security consultant company that specializes in software penetration testing.

Static Code Scanning

Skybox performs static code analysis on its source code to highlight possible vulnerabilities within "static" (i.e., non-running) source code. Scans are performed per commit, nightly and quarterly.

High-Profile Vulnerabilities

If a high-profile vulnerability is published for a common system component (such as SSL or SSH), Skybox will analyze the possible impact of this vulnerability within 48 hours and will publish a Security Advisory with analysis and suggested remediation steps if the vulnerability affects the Skybox Application or Appliance (see details below).

Additional Sources

Vulnerabilities reported by Skybox users or security consultants will be immediately analyzed by Skybox as described above.

Reporting Security Issues

To report a security issue please contact <security@skyboxsecurity.com>.

Vulnerability Remediation SLA

Vulnerabilities with high or critical CVSS (v3) scores or with critical impact receive immediate attention and will be fixed as soon as possible.

Vulnerability Severity	Response Time
Critical (CVSS 9 and higher)	Up to 15 days *
Medium to High (CVSS 5-9)	Up to 90 days *
Low (CVSS 1-5)	Up to 120 days *

* Fixes to vulnerabilities affecting the Appliance OS depend on the availability of fixes by the CentOS community or official package owners.

Vulnerability Publishing

Security Advisory

Skybox will publish a Security Advisory for critical or high-profile vulnerabilities.

The advisory will include information about the vulnerability and its impact on the Skybox Application or Appliance. The advisory will list the affected versions and guidelines for remediation.

Even if a critical or high-profile vulnerability has no impact on the Skybox Application or Appliance, Skybox will publish the advisory to explain *why* the vulnerability has no impact on Skybox products.

The Security Advisory will be available in the Skybox Knowledge Base.

Security Fix List

Skybox Release Notes for new Skybox releases will include a list of all security fixes since the previous release.