SKYBOX SOFTWARE SECURITY PUBLICATION POLICY

INFORMATION ON SKYBOX® SECURITY VULNERABILITY DETECTION AND PUBLISHING PROCESSES

December 2019

SKYBOX® SECURITY

1. POLICY OVERVIEW

The purpose of this document is to describe the policy, process and measures Skybox Security takes to verify that our products are secure and not exposed to vulnerabilities. This document also describes the response, remediation and publishing processes if a vulnerability is found.

2. 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 application and appliances.

The processes described in this document apply to the Skybox application, appliance web admin and appliance Linux packages.

2.1 Vulnerability Scan

Current Skybox application and appliance products are scanned every eight weeks to identify third-party library vulnerabilities that have been published and exist on the platform since last scan.

2.2 Penetration Testing

Skybox conducts penetration testing for both Skybox application and appliances to identify new vulnerabilities.

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

2.3 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.

2.4 High-Profile Vulnerabilities

If a high-profile vulnerability is published for a common system component (e.g., SSL, 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).

2.5 Additional Sources

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

3. VULNERABILITY RESPONSE TIMES

If a potential vulnerability is detected or reported, Skybox will analyze the vulnerability, possible exploit level and risk to the Skybox application and appliance.

Skybox will remediate the vulnerability per the service level agreement (SLA) defined below and provide remediation guidelines.

3.1 Vulnerability Remediation SLA

Based on industry best-practices, Skybox handles all vulnerabilities according to their severity. Most vulnerabilities should be handled according to the following table. If for some reason, a vulnerability cannot be fixed within the expected response time, we will provide analysis and ETA for such vulnerability.

VULNERABILITY SEVERITY	RESPONSE TIME
Critical (CVSS 9.0-10.0)	**Up to 15 days**
High (CVSS 7.0-8.9)	**Up to 30 days**
Medium (CVSS 4.0-6.9)	**Up to 90 days**
Low (CVSS 0.1-3.9)	**Up to 120 days**

3.2 Vulnerability Publishing

3.2.1 SECURITY ADVISORY

Skybox will publish a security advisory for critical- and high-profile vulnerabilities.

The advisory will include information about the vulnerability and its impact on the Skybox application or appliance. The advisory will detail affected versions and guidelines for remediation.

The security advisory will be available in the Skybox Knowledge Base.

3.2.2 SECURITY FIXES LIST

Release notes for new Skybox releases will include a list of all security fixes made from the time of previous release.