Hammerspace Vulnerability Remediation SLA

Version 5.3

HAMMERSPACE

Table of Contents

About This Documentation

This document is a security communication describing Hammerspace, Inc.'s service-level agreements (SLAs) for remediating or mitigating security vulnerabilities in Hammerspace software, and how to report a product security concern. It is informational and is not a configuration or administration guide.

© 2026 - Hammerspace

Chapter 1. Reporting a Product Security Concern

To report a security concern, please contact Hammerspace Support.

© 2026 - Hammerspace

Chapter 2. VULNERABILITY REMEDIATION SLAs: Hammerspace Data Platform

The information in this document, including products and software versions, is current as of the release date. This document is subject to change without notice.

Last Updated: 2026-01-20

2.1. DESCRIPTION

These **Vulnerability Remediation SLAs** define the maximum time allowed between the identification of a security vulnerability and the implementation of a remediation or approved mitigating control.

Identifying a security vulnerability involves systematically finding flaws (like bugs, misconfigurations, or missing patches) in systems, networks, and applications that attackers could exploit for unauthorized access or damage, typically done through automated tools like scanners, penetration testing, audits, threat intelligence, and manual analysis to assess security posture and prioritize remediation

Vulnerabilities are prioritized based on impact and exploitability, with increased priority for Internet-exposed and security-sensitive components. Compliance with these SLAs is monitored and tracked as part of Hammerspace's secure development and operations processes.

Severity	Definition	Remediation SLA
Critical	Actively exploitable or severe impact	≤ 72 hours
High	High impact, no known active exploit	≤ 14 days
Medium	Moderate impact	≤ 30–60 days
Low	Low impact or informational	≤ 90 days

The remediation timeline begins upon confirmation of vulnerability applicability to the Hammerspace Data Platform components. Remediation may include patching, configuration changes, or implementation of compensating controls where patching is not immediately feasible. Exceptions require documented risk acceptance and management approval and are reviewed periodically.

©Copyright 2026 Hammerspace, Inc.

Hammerspace shall not be liable for technical or editorial errors or omissions contained herein. The information provided is provided "as is" without warranty of any kind. To the extent permitted by law, neither Hammerspace nor its affiliates, subcontractors or suppliers will be liable for incidental, special or consequential damages including downtime cost; lost profits; damages relating to the procurement of substitute products or services; or damages for loss of data, or software restoration. The information in this document is subject to change without notice.

Hammerspace and the names of Hammerspace products referenced herein are trademarks of Hammerspace in the United States and other countries. Other product and company names mentioned herein may be

trademarks of their respective owners