SecuriTy gOveRnance Management

2024-05-30

Cybersecurity Policy - Vulnerability Disclosure

Emmanuel P CAPITAINE
Director Infrastructure & Security
OnLogic
35 Thompson St
South Burlington, VT 05403

Diffusion: Confidential
Recipients: L0 - Executive
L1 - Directors
L2 - Managers

Version 1.0

TABLE OF CONTENT

TABLE OF CHANGES

Version	Date	Author	Description
1.0	2024-05-30	Emmanuel P CAPITAINE	Document creation

Overview

OnLogic is committed to protect its customers against any cybersecurity that might affect any of our products and services. OnLogic is therefore committed to provide timely information and mitigation options to address vulnerabilities.

Purpose

The purpose of a vulnerability disclosure policy is to establish a clear and trusted method for security researchers to report vulnerabilities related to OnLogic products. It outlines the following:

- **Encourages responsible reporting:** The policy aims to incentivize security researchers to disclose vulnerabilities directly to OnLogic rather than through public channels or exploiting them for malicious purposes.
- **Improves security posture:** By receiving vulnerability reports, OnLogic can prioritize and fix security weaknesses, ultimately making our products more secure.
- **Defines communication channels:** The policy establishes clear communication channels for researchers to submit vulnerability reports and for OnLogic to provide updates on the remediation process.
- **Sets expectations:** Both OnLogic and the security researcher understand their roles and responsibilities throughout the vulnerability disclosure process.

Severity

OnLogic uses Version 3.1 of the Common Vulnerability Scoring System (CVSS) as part of the evaluation process for product vulnerabilities. The main purpose of the Common Vulnerability Scoring System (CVSS) is to provide a standardized way to assess the severity of security vulnerabilities in computer systems. It assigns a score (0-10) based on various metrics that reflect how easy it is to exploit a vulnerability and the potential impact it can have.

OnLogic summarizes the assessed impact of a vulnerability by way of a numeric score, vector string and qualitative representation of the severity (i.e., one of Critical, High, Medium, Low), as per the scale provided below

Severity	CVSS v3.1 Score
Critical	9.0 – 10
High	7.0 – 8.9
Medium	4.0 – 6.9
Low	0.1 – 3.9

Vulnerability Reporting

OnLogic works continuously to identify and limit the risk associated with vulnerabilities in our products. If you identify a security vulnerability, please report the problem immediately. Security vulnerabilities related to open-source software components should be addressed directly to the responsible entity.

Please submit a report to security@onlogic.com with the following information:

- Product name and version containing the suspected weakness / vulnerability;
- Technical information about the potential vulnerability.
- Steps to reproduce.
- Estimated CVSS v3.1 score rating and resulting vector string.
- A remediation suggestion.
- The researcher's own vulnerability disclosure policy if available.

Product Security Incident Response

The OnLogic Product Security Incident Response Team (PSIRT) is responsible for responding to OnLogic products security incidents. The OnLogic PSIRT is a global team managing the receiving, investigation and public reporting of information about security vulnerabilities.

The psirt@onlogic.com email address is intended ONLY for the purpose of reporting product or service vulnerabilities. For technical support information on our products or services, please visit our support site support.onlogic.com

Remediation

The OnLogic security teams upon discovery of a vulnerability will assess impact on our product line.

Remediation of the vulnerability will depend on factors such as

- Severity of the vulnerability
- Complexity of the vulnerability
- Scope of the affectedness
- Effort and impact of remediate
- Product Life Cycle

Once a patched version is available, it will be rigorously tested to ensure that the change will not affect the product operationess. Validated patches will be made available on the security advisories web page for all OnLogic customers.

Security Advisory

OnLogic security advisory is publicly available at www.onlogic.com/security/advisories.

Third party notifies OnLogic of a potential vulnerability found in our products. OnLogic will investigate the finding and may publish a coordinated disclosure along with the third party.

OnLogic may receive information about a security vulnerability from a supplier under a confidentiality or non-disclosure agreement or under embargo. In these cases, OnLogic will work with the supplier to request that a security fix is released although we may not be able to provide details about the security vulnerability.

Disclaimer

All aspects of this Vulnerability Response Policy are subject to change without notice. Response is not guaranteed for any specific issue or class of issues. Your use of the information in this document or materials linked herein is at your own risk.

Last page left blank intentionally