INSOMNIA

SECURITY SPECIALISTS :: REST SECURED

PROJECT EXECUTIVE REPORT

OCTOPUS DEPLOY SAAS SECURITY REVIEW

Octopus Deploy Pty. Ltd.

PO Box 308
Indooroopilly
QLD 4068
Australia

Insomnia Security Group Ltd.

PO Box 39803
Auckland 2145
New Zealand

Auckland office: +64 (0)9 972 3432
Wellington office: +64 (0)4 974 6654

Project	Octopus Deploy SaaS Security Review	**Reference**	OCT:ODS/1805
Publication Date	15 June 2018	**Version**	1.1 Release

Date	Version	Change	By
28 May 2018	0.1	Draft	Lim Ke
29 May 2018	0.2	Internal QA	Ben Knight
30 May 2018	1.0	Document Published	Brett Moore
15 June 2018	1.1	Document Updated	Paul Campbell

Legal Statement

Every effort has been made to ensure that the information contained in this document is true and correct at the time of publication. However, the products, specifications, and content in general that are described in this document are subject to continuous development and improvement, and therefore Insomnia Security cannot accept liability for any loss or damage of any nature whatsoever arising or resulting from the use of or reliance on outdated information or particulars.

Insomnia Security does not warrant that the material contained in this documentation is free of errors. Any errors found in this document should be reported to Insomnia Security in writing.

Insomnia Security warrants that this security review has been done using all relevant tools, methods and techniques available and known by the testers at the time of this review. However, due to the nature of computer/network/application security, we cannot guarantee that all security related issues have been identified.

Confidentiality

The information in this document is confidential and meant for use only by the intended recipient. The material contained in this document represents information pertaining to products and methods in use by us.

By taking receipt of this document, the receiving party agrees that the information in this document shall not be used, or disclosed for any purpose other than that which it is provided for without first obtaining written consent from Insomnia Security.

Document Information

This Report contains the results of security testing performed during the Octopus Deploy Pty. Ltd. Octopus Deploy SaaS Security Review between the 17th of May and the 14th of June 2018.

This Insomnia Security Report has been delivered as two separate documents:

- **Executive Report (this Report):** A high-level overview of the testing results, aimed at executives and project management.
- **Technical Report:** A detailed view of the testing results, including technical recommendations for resolving the discovered issues, aimed at technical staff charged with remediation work.

Table of Contents

Executive Summary **5**

Engagement Summary **6**

Findings Summary **7**

Vulnerability Risk Rating 7

Severity of Exploitation 7

Likelihood of Exploitation 7

Vulnerability Rating Definitions **8**

Executive Summary

Insomnia Security was engaged to perform a security review of the Octopus Deploy automated deployment product. This was performed as a part of efforts by Octopus Deploy Pty. Ltd. to ensure that the new product deployment to the AWS environment does not result in the exposure of new security vulnerabilities.

The on-premise deployment of Octopus Deploy has been previously reviewed by Insomnia Security and this current review also included regression testing of some of the previously reported findings. In addition, testing of the web application review as an unauthenticated and an authenticated user, network vulnerability scanning against the external facing portal and a network review against the internal environment from the perspective of a compromise host. Additionally, Insomnia Security performed application level review against key features such as the “Run a Script” feature to execute commands on the instance itself.

The security review identified one minor issue in Octopus Deploy that should be addressed to further improve the security of the product and two low risk issues that are included for informational purposes.

Overall, the Octopus Deploy product in the AWS environment does not introduce any significant vulnerabilities and the remediation actions taken to address the previously identified issues have adequately resolved the previously discovered medium risk issues.

It is recommended that the items included in the report are reviewed internally, and the appropriate remediation action planned where deemed necessary. Insomnia Security is available to carry out regression testing as required, once any issues have been resolved.

Insomnia Security considers the subject of the Octopus Deploy SaaS Security Review to pose a business risk at the level of:

MINOR

An overview of Insomnia Security’s findings, showing the number and severity of each of the identified security related issues, can be found in the ‘Findings Summary’ section of this Report.

Engagement Summary

This section contains a summary of findings of the security testing performed during the Octopus Deploy Pty. Ltd. Octopus Deploy SaaS Security Review between the 17th of May and the 14th of June 2018. Please refer to the accompanying Technical Report, which outlines each vulnerability in detail, along with recommendations for remediation.

Insomnia Security was engaged to perform a security review of the Octopus Deploy automated deployment product. This was performed as a part of efforts by Octopus Deploy Pty. Ltd. to ensure that the new product deployment to the AWS environment does not contain the previously discovered issues and the AWS integration does not introduce new vulnerabilities into their customers' deployment environments.

According to the agreed scope, the security review specifically focuses on testing the following areas:

- Automated network vulnerability scanning against the testing instance from the Internet.
- Application level review against the end user web interface and API as unauthenticated user.
- Misuse the "Run a Script" feature to execute commands on the instance in order to assess the script runner's user permission.
- Verify what can be accessed if a deployment server instance was compromised via a provided RDP session.
- Regression testing against the previously discovered vulnerabilities.

The application review as an unauthenticated attacker did not discovered common web application vulnerabilities including cross site scripting, SQL injection and other issues commonly referred to as the OWASP Top 10.

The application review as an authenticated attacker included testing of the "Run a Script" feature which confirmed that while it was possible to execute commands, these commands are now executed under a low privilege user (svcscriptrunner) account. This mitigation prevents the exposure that previously existed, and would require an attacker to discover a privilege escalation flaw to gain further access.

Automated network scanning discovered a number of commonly seen SSL configuration issues. These findings are included in the Technical Report for informational purposes

Utilising the RDP session to connect to an Octopus Server Instance, Insomnia Security performed network scanning and reconnaissance against the internal network. As a result, a number of hosts were found to be reachable in the internal network, presenting the attacker a list of potential further targets in the situation of the compromise of an Octopus Server Instance. The details of the network discovery and reconnaissance results have been included in the Appendix section in the Technical Report.

This testing did however confirm that the implemented firewall rules (security groups) were enforced and in place as documented.

The regression testing of the included issues that were previously reported, were mostly found to have been adequately resolved and to not introduce any further flaws.

Overall, the Octopus Deploy product in the AWS environment does not introduce any significant vulnerabilities and the remediation actions taken to address the previously identified issues have adequately resolved the previously discovered medium risk issues.

It is recommended that the items included in the report are reviewed internally, and the appropriate remediation action planned where deemed necessary. Insomnia Security is available to carry out regression testing as required, once any issues have been resolved.

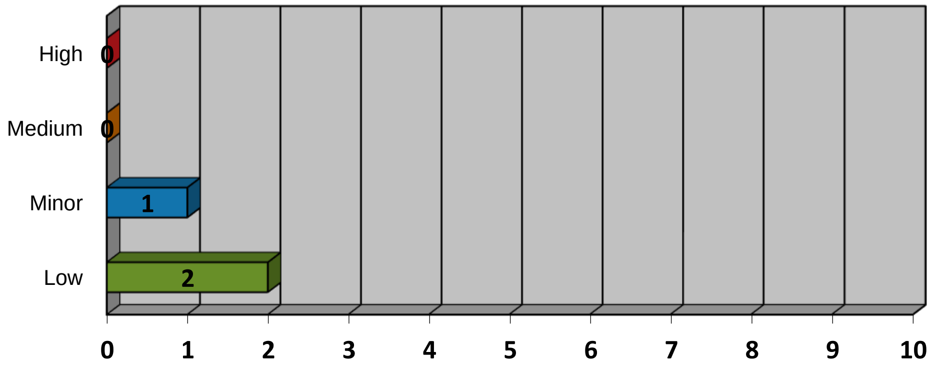
Insomnia Security considers the subject of the Octopus Deploy SaaS Security Review to pose a business risk at the level of: MINOR

An overview of Insomnia Security's findings, showing the number and severity of each of the identified security related issues, can be found in the 'Findings Summary' section of this Report.

Findings Summary

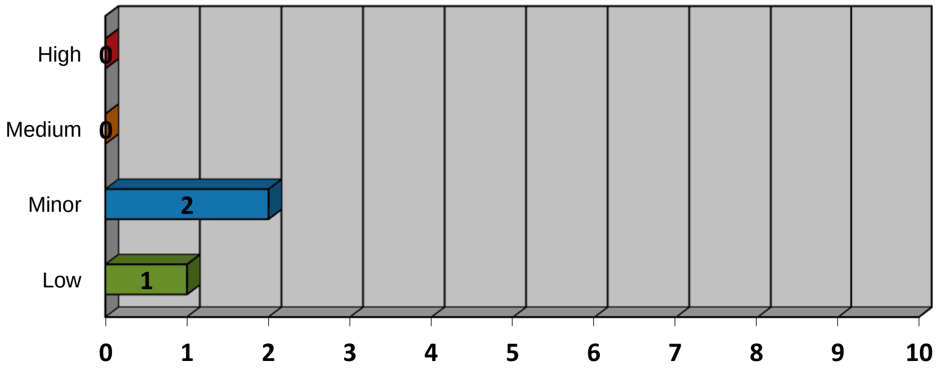
Vulnerability Risk Rating

The following risk rating is based on the severity and likelihood ratings of a reported issue, and provides an indication of the risk the business is being exposed to:



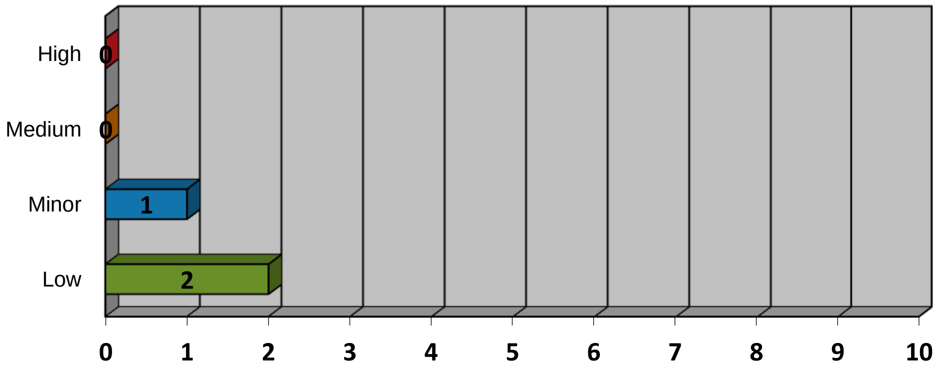
Severity of Exploitation

The following severity rating is based on the consequences if the above vulnerability was exploited to its fullest potential by a person with all the required knowledge and information:



Likelihood of Exploitation

The following likelihood rating is based on the ease in which the vulnerability could be exploited, taking into account those factors relating to how the vulnerability could be discovered and accessed by a person external to the company:



Vulnerability Rating Definitions

Insomnia Security endeavours to provide the most appropriate ratings for the issues identified during the review. Ratings are based on various aspects around the context of the vulnerability, and the industry in which the customer operates.

Severity Rating

The severity rating is based on the consequences of the issue. That is, if the vulnerability was exploited to its fullest potential by a person with all required knowledge and information.

LOW	**Exploitation of this vulnerability would cause little or no damage** This type of vulnerability may be an information disclosure issue, which would not reveal enough information to cause any damage.
MINOR	**Damage caused by this vulnerability would be relatively negligible and limited in scope** This type of vulnerability may disclose information that, although not extremely sensitive, should not be available to an attacker.
MEDIUM	**Exploitation of this vulnerability would be bad for a customer's reputation** This type of vulnerability may affect a small number of users, and could have moderate financial or legal implications. These issues may lead to the exposure of customer data or credential information.
HIGH	**Vulnerabilities in this category would be very bad for a customer's reputation** This type of vulnerability may affect a large number of users, and could have serious financial or legal implications. These issues may lead to the total control of affected servers, applications, or network devices.

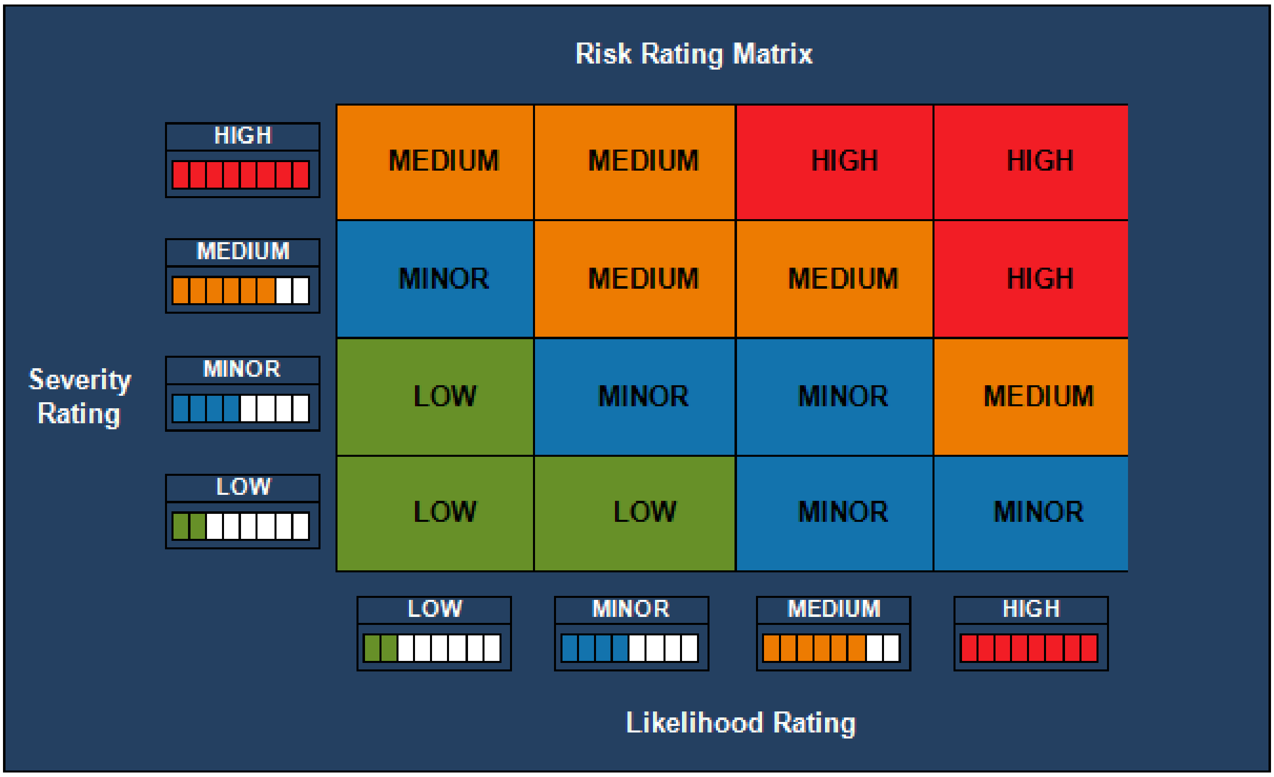
Likelihood Rating

The likelihood rating is based on the ease in which the vulnerability could be exploited, as well as taking into account the factors related to how the vulnerability could be discovered and accessed by a person external to the customer's company.

LOW	**Extremely difficult to write a working exploit for** Would require a large amount of internal knowledge, and very unlikely to be discovered remotely.
MINOR	**Very difficult to exploit** Administrative authentication or multiple credentials would probably be required.
MEDIUM	**The attacker must write their own exploit** Some internal information or user level authentication would be required.
HIGH	**Very easy to discover and exploit remotely** Likely a well-known vulnerability with an exploit readily available, or no authentication required.

Risk Rating Chart

The following chart was used as a guideline when Insomnia Security calculated the eventual risk rating for the issues identified during the review:



Risk Rating Matrix

Severity Rating	LOW	MINOR	MEDIUM	HIGH
HIGH	MEDIUM	MEDIUM	HIGH	HIGH
MEDIUM	MINOR	MEDIUM	MEDIUM	HIGH
MINOR	LOW	MINOR	MINOR	MEDIUM
LOW	LOW	LOW	MINOR	MINOR

Likelihood Rating

INSOMNIA

SECURITY SPECIALISTS :: REST SECURED