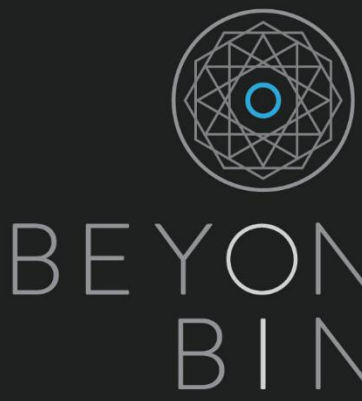

BEYOND BINARY

Annual Security Assessment

Octopus Deploy

ANNUAL SECURITY ASSESSMENT

PREPARED FOR

Jim Burger, Director, Trust and Security, Octopus Deploy

Kyle Jackson, Senior Security Engineer, Octopus Deploy

PREPARED BY

OJ Reeves, Director, Beyond Binary

Rick Oates, Authorised Intruder, Beyond Binary

Ashley Donaldson, Authorised Intruder, Beyond Binary

Ryan Catterall, Authorised Intruder, Beyond Binary

VERSION

1.0

DATE SUBMITTED

9 August 2021

EXECUTIVE SUMMARY

As part of a proactive security program, Beyond Binary was engaged by Octopus Deploy to conduct an annual security assessment over a three-week period. The primary goals of the engagement were to:

- Review the package management system utilised by Octopus;
- Examine a subset of APIs used by the Octopus product;
- Assess the Halibut protocol leveraged between servers and tentacles;
- Perform social engineer attacks via different mediums such as Slack and email;
- Determine if any vulnerabilities exist in the worker functionality of the Octopus application.

A total of 6 issues were discovered, one of which was rated as high-risk, and one of which was rated as moderate risk. The most severe issue, remote code execution in the Halibut protocol, if exploited, could allow an attacker to achieve code execution on older versions of Octopus server. Recent changes within the Octopus Deploy server have made this difficult more difficult to undertake in the real world, however older versions of the software are vulnerable.

Beyond Binary would like to note that based off this assessment, it was observed that Octopus Deploy has a limited attack surface from an unauthenticated perspective. Users were security aware and reported phishing attempts as they happened. A single user clicked on a phishing email during the engagement and recommendations have been made to reduce the risk of this occurring in the future.

In summary, Beyond Binary would grade the security posture of the in-scope systems as follows:

RISK RATINGS EXPLAINED

All findings in this report have been assigned an overall risk rating according to the following table; please note Beyond Binary's risk rating system may not align completely with your organisation's risk rating system.

Risk Rating	Description
Extreme	Exploitation of the vulnerability is straightforward and results in complete compromise of servers or infrastructure devices and the most sensitive business information. Remediation of critical-risk findings should be initiated immediately.
High	Upon exploitation of the vulnerability, an attacker would have the ability to severely adversely affect organisational operations, obtain sensitive information and alter records. Remediation of high-risk findings should be initiated immediately.
Moderate	The vulnerability might enable an attacker to cause degradation to the organisation's operations or obtain non-sensitive information; it is either difficult to exploit, or it would need to be used in conjunction with another vulnerability to gain privileged access, or to affect confidentiality, integrity or availability.
Low	The vulnerability provides information the attacker could use to build a dossier on the organisation in preparation for further attacks or it reduces security in a way that does not immediately impact the organisation.
Informational	These management letter points describe information that was deemed relevant to the security of the organisation. While they do not currently pose an immediate security issue, they should be investigated further to ensure related vulnerabilities have not been overlooked.

Likelihood \ Impact	Low	Medium	High	Critical
High	Moderate	High	High	Extreme
Medium	Low	Moderate	High	High
Low	Low	Low	Moderate	High

SUMMARY OF FINDINGS

The following findings have been identified:

	Critical	High	Moderate	Low	Total
Findings	0	1	1	4	6

Finding	Risk Rating
Remote Code Execution via Deserialisation in Halibut Protocol	High
Ability to call additional methods	Moderate
License Signature Bypass	Low
Ability to run code on Octopus Cloud	Low
Services in other containers accessible	Low
Able to exceed user invitation limit	Low

SECURITY STRENGTHS

Security assessment reports tend to focus solely on the issues discovered, and hence almost always have a negative slant. At Beyond Binary we also believe in identifying and recognising areas where the target of the assessment performed well from a security standpoint. The following points were highlighted as quality implementations that helped prevent further attack:

- Limited Attack Surface – The APIs and package management system of Octopus had a very limited attack surface from an unauthenticated perspective. This shows a robust security design combined with an active patching schedule.

- Security Aware Users – Octopus employees have demonstrated security awareness through both Slack and email mediums. Users did not add an employee to authenticated groups even when requested to by the employee. Users reported the phishing email to the appropriate channels upon receipt.

Annual Security Assessment 2021

Management Response

Author: James Burger, Director of Trust & Security Operations

Executive Summary

On the 9th August 2021, Beyond Binary completed a comprehensive review of the development process and attack surface area of Octopus Deploy, focusing on key risk areas identified during previous engagements.

Primarily this was focussed on several areas:

- Octopus Cloud worker security
- Application security of the Octopus API
- Application security of the communication protocols used between server and client (Halibut)
- Our software supply chain and build / packaging process
- Our staff's susceptibility to social engineering attacks via various channels

We identified 6 issues as described in the assessment, and we have addressed each issue, in some cases via patches to the current versions of our software. These patches were delivered to customers well within 90 days of discovery by Beyond Binary. To date, we have no evidence that these vulnerabilities were exploited in the wild.

We also self report these (and other) vulnerabilities that are found in our product to Mitre, as part of our involvement as a CNA in the CVE process, and publish notifications to our customers via https://advisories.octopus.com

We remain committed to high standards of application security and communication to our customers with regards to vulnerabilities, exploits and data breaches associated with Octopus Deploy products and services.

Date: 11th November 2021

Signed:

DocuSigned by:

James Burger

F8B14527E2414A7...

James Burger, Director of Trust & Security Operations