BEYOND BINARY

Annual Security Assessment

Octopus Deploy

ANNUAL SECURITY ASSESSMENT

PREPARED FOR

Jim Burger, Director, Trust and Security, Octopus Deploy

Kyle Jackson, Security Operations Manager, 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

19 September 2022

EXECUTIVE SUMMARY

As part of a proactive annual security program, Octopus Deploy engaged Beyond Binary to evaluate a range of security products and infrastructure utilised within the organisation. What Beyond Binary found was a mature, well hardened set of applications with few to any issues.

The Octopus Server and Tentacle products were a focus of testing and found to have no significant security issues. Minor recommendations have been made surrounding web headers used by the application. This assessment included retesting previously identified issues which were found to have been remediated successfully.

The Slipway and Step Package Public Feed were assessed and found to have no major security issues. One theoretical attack was proposed against the Step Package Public Feed however there is no indication that Octopus is vulnerable given their current configuration.

A high-level overview was undertaken of the build system and Beyond Binary could not identify any significant risks within the current workflow. Finally, some minor security best practice violations were identified in SEQ, an application that Octopus Deploy uses rather than has developed themselves. These best practice violations do not pose any direct threat to Octopus Deploy.

Beyond Binary would like to commend Octopus Deploy on an excellent security result, with it rare for an organisation to have such limited findings during an assessment.

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
Critical	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.
Medium	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	Medium	High	High	Critical
Medium	Low	Medium	High	High
Low	Low	Low	Medium	High

SUMMARY OF FINDINGS

The following findings have been identified:

	Critical	High	Medium	Low	Total
Findings	0	0	0	3	3

Finding	Risk Rating
Vulnerable JavaScript Dependency (Moment.js)	Low
Weak Content Security Policy Header	Low
User Controlled Key Selection in Package Upload	Low
Detailed Unauthenticated Version Enumeration	Informational

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:

- Role Based Access Control – The Octopus model utilises role-based access control to ensure only those with sufficient permissions can perform dangerous actions. Beyond Binary did not discover any method of bypassing or subverting this role-based access control.
- Use of LINQ where possible – The Octopus code base, in its numerous repositories, utilised LINQ when performing queries or data manipulation. This avoided more dangerous techniques such as string manipulation which is more prone to being subverted via malicious inputs.
- Mature Organisation – The organisation's approach to security is mature and the code examined exhibited good security hygiene. Very few dangerous methods were utilised within the application, there were no discernible logical flaws, and rigorous test cases are throughout the codebase.
- Security Best Practices – It is rare that during an assessment a significant number of "best practice" security issues are not discovered. Octopus Deploy clearly adheres to security principles as even low risk issues were scarce, and even then, often occurred in code not directly controlled by Octopus Deploy.