BEYOND BINARY

Web Application and Attack Simulation Security Assessment Report

Octopus Deploy

BEYOND BINARY
AUTHORISED INTRUSION
+61 431 952 586
CONTACT@BEYONDBINARY.IO
BEYONDBINARY.IO

WEB APPLICATION AND ATTACK SIMULATION SECURITY ASSESSMENT REPORT

PREPARED FOR

Jim Burger, Principal Data Protection Officer, 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

Michael Bielenberg, Authorised Intruder, Beyond Binary

VERSION

1.0

DATE SUBMITTED

5 September 2023

EXECUTIVE SUMMARY

As part of a proactive security program, Beyond Binary was engaged by Octopus to conduct a Web Application Assessment of the Octopus cloud, to discover any security flaws that could impact Octopus or its clients. In addition, several common attack scenarios were tested, such as phishing, and cryptocurrency mining.

The overall quality of the applications assessed was excellent. No serious vulnerabilities were identified in the web application, however some minor issues were found.

GOALS

The primary goals of the engagement were to:

- Discover and document any security flaws that an Internet-facing attacker could exploit, that could cause harm to Octopus or its clients.
- Determine the risk and potential impact on the business as a result of having those flaws.
- Provide a set of recommendations that will aid in remediating the issues that were discovered.

The web applications were assessed using a combination of custom assessment methods and the guidelines laid out in the standardized OWASP Testing Guide.

RESULTS

A total of 4 issues were discovered, 1 of which was rated as medium-risk, and 3 of which were rated as low-risk issues. The medium-risk issue was a logic error that nearly resulted in an account compromise vulnerability but was unexploitable in practice.

The three phishing campaigns were successfully defended against, with automated systems preventing some emails, and staff awareness and reporting preventing others. One of the three goals was partially achieved.

Beyond Binary would like to note that based off this assessment, it was observed that the application developers have made every effort to reduce their threat footprint and embrace frameworks and their associated technologies to build robust security into their application.

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

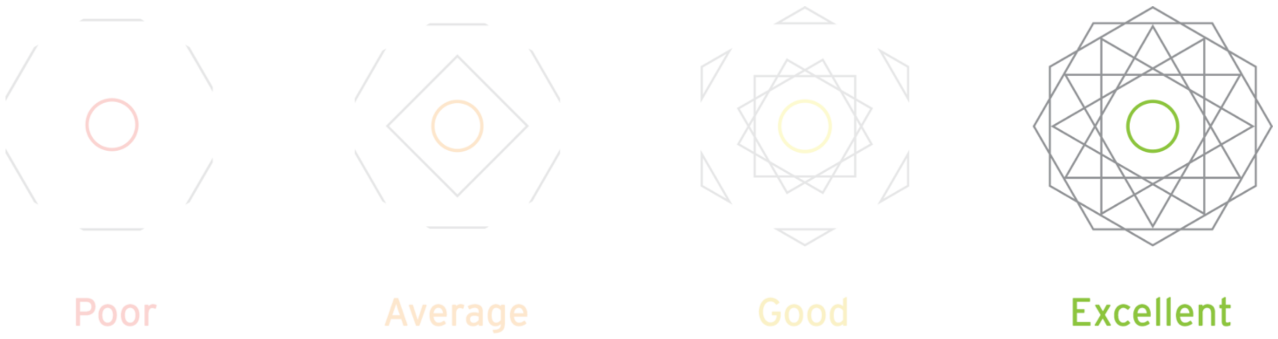

TABLE OF CONTENTS

SCOPE 5
- URLs In Scope 5

RISK RATINGS EXPLAINED 6

SUMMARY OF FINDINGS 7

OWASP SCORECARD 8

EFFECTIVE SECURITY CONTROLS 9

ENGAGEMENT OVERVIEW 10
- Octopus ID 10
- Octopus Cloud Portal 10
- Customer Control Centre 10
- Dynamic Workers Leasing API 10
- Cloud Instances 11
- Octofront 11
- Azure and Entra AD 11
- Attack Simulations 11
  - Crypto-mining 11
  - Deployment Disruption 12
- Phishing Campaigns 13
  - Campaign 1: Account Compromise 13
  - Campaign 2: Targeting Engineers 16
  - Campaign 3: Targeting Support Team 17

DETAILED FINDINGS 20
- Medium Risk Findings 20
  - MessageSigner Type Confusion risk 20
- Low Risk Findings 25
  - Cross-Site Request Forgery in admin panel 25
  - Worker Persistence – System Service 27
  - Octopus ID Current Password Change Bypass 28
- Informational Findings 29
  - Risky serialisation settings 29
  - Worker Persistence – RDP Access 31
  - HTML Injection in Cloud Instance 33

CONCLUSION 35

SCOPE

The assessment specifically targeted the online Octopus application stack. Any other applications associated with the platform(s) were considered out of scope.

URLS IN SCOPE

Application	URL
Octopus ID/Control Centre v1	https://preprod.octopus.com
Control Centre v2	https://billing.octopushq.com
Cloud Portal	https://preprod-cloud.octofront.com
Cloud Instance	https://pentest202308.testoctopus.app
Dynamic Worker Leasing API	https://leasingapi-preprodpentest.azurewebsites.net
Octofront	https://preprod.octofront.com

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.

		Impact			
		Low	Medium	High	Critical
Likelihood	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	1	3	4

Finding	Risk Rating
MessageSigner Type Confusion risk	Medium
Cross-Site Request Forgery in admin panel	Low
Worker Persistence - System Service	Low
Octopus ID Current	Low
Risky serialisation settings	Informational
Worker Persistence - RDP Access	Informational
HTML Injection	Informational

OWASP SCORECARD

This scorecard is intended to give a high-level view of the security of the Internet-facing site.

Top 10 Name	Description	Pass / Fail
A01 – Broken Access Control	Restrictions on what authenticated users are allowed to do are often not properly enforced. Attackers can exploit these flaws to access unauthorized functionality and/or data, such as access other users' accounts, view sensitive files, modify other users' data, change access rights, etc.	✓ Pass
A02 – Cryptographic Failures	Cryptography should be used to protect data in transit and at rest. Web applications need to ensure that cryptography is used where needed, according to best practice, and does not itself introduce new vulnerabilities.	✓ Pass
A03 – Injection	Injection flaws, such as SQL, Command, JavaScript (XSS) and LDAP injection, occur when untrusted data is sent to an interpreter as part of a command or query. The attacker's hostile data can trick the interpreter into executing unintended commands or accessing data without proper authorization.	✓ Pass
A04 – Insecure Design	The design of a system influences its security as much as its implementation. Solid design principles should be followed to ensure that logic flows have considered the possibility of abuse, that components are used only for their intended purpose, and that features to support good security principles are present within the system.	✓ Pass
A05 – Security Misconfiguration	The security of systems can be undermined by their configuration; for example, using default credentials, incomplete or ad hoc configurations, open cloud storage, HTTP headers, and providing verbose error messages containing sensitive information.	✓ Pass
A06 – Vulnerable and Outdated Components	Components, such as libraries, frameworks, and other software modules, run with the same privileges as the application. If a vulnerable component is exploited, such an attack can facilitate serious data loss or server takeover. Applications and APIs using components with known vulnerabilities may undermine application defences and enable various attacks and impacts.	✓ Pass
A07 – Identification and Authentication Failures	Application functions related to authentication and session management are often implemented incorrectly, allowing attackers to compromise passwords, keys, or session tokens, or to exploit other implementation flaws to assume other users' identities temporarily or permanently.	✓ Pass
A08 – Software and Data Integrity Failures	Applications that incorporate functionality (e.g., plugins, web services, templates, or serialized data) from 3rd parties or from users should verify the authenticity and integrity of these components. This includes in CI/CD pipelines. Failure to do so can allow attackers to execute code on servers or access sensitive resources.	✓ Pass
A09 – Security Logging and Monitoring Failures	Security logs, when integrated with monitoring solutions, can greatly assist in detecting attacks or successful breaches. Inadequate logs, or the ability for an attacker to corrupt or avoid logs, can allow them to abuse the system for longer without detection, and can complicate incident response after the fact.	N/A
A10 – Server-Side Request Forgery	SSRF vulnerabilities allow an attacker to coerce a system into making a request to a resource on their behalf, usually on an internal network that is otherwise inaccessible to the attacker. This can allow accessing sensitive data or exploiting other vulnerabilities on the internal network.	✓ Pass

EFFECTIVE SECURITY CONTROLS

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:

- Robust software design – The quality of the code was very high, with clear responsibilities for most classes, and easy-to-follow code. Software vulnerabilities often arise amidst complex code, so the clarity of Octopus's code is a contributor to the low number of vulnerabilities found in the codebase.
- Use of frameworks – Vulnerabilities often occur at the boundary between technologies. Octopus extensively used frameworks such as Razor templating engine and Azure Identity to better secure these transitions.

CONCLUSION

The overall quality of the in-scope systems from a security standpoint is excellent. Octopus Deploy clearly prioritises security in their software development processes, resulting in a relatively low number of findings given the size of the codebase. There are a number of issues that need attention, however, the attack team is confident that the work involved will not take an extensive period of time.

Beyond Binary was delighted to be given the opportunity to provide this security assessment service to the team at Octopus Deploy. We appreciate the continued business relationship and hope to be able to provide other security-related services again in the near future should Octopus Deploy require them.

If any clarification is required, please don't hesitate to contact me personally on oj@beyondbinary.io or +61 431 952 586.

Thank you and best regards on behalf of the Beyond Binary team,

OJ Reeves
Founder and Authorised Intruder
Beyond Binary Pty Ltd