Octopus Deploy

Helping secure customers by disclosing more

Kyle Jackson
AusCERT 2022

Hi I'm Kyle 👋

🏢 Security Operations Team Lead at Octopus Deploy

Contact Information:

Email - kyle.jackson@octopus.com

LinkedIn - https://au.linkedin.com/in/kyle-jackson-14ab30101

GitHub - https://github.com/wizedkyle

Why disclose software vulnerabilities?

Help ensure your customers stay secure!

Why doesn’t everyone disclose vulnerabilities?

Just a few reasons……

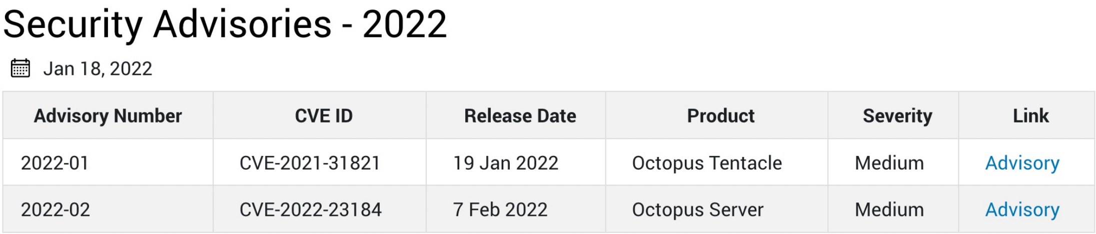
Our product may be exploited if we publicly disclose our vulnerabilities

Our customers can’t easily patch their environments, or they don’t patch their environments

We will get bad press if we tell people about software vulnerabilities in our product

Disclosing vulnerabilities isn’t something the business has thought about

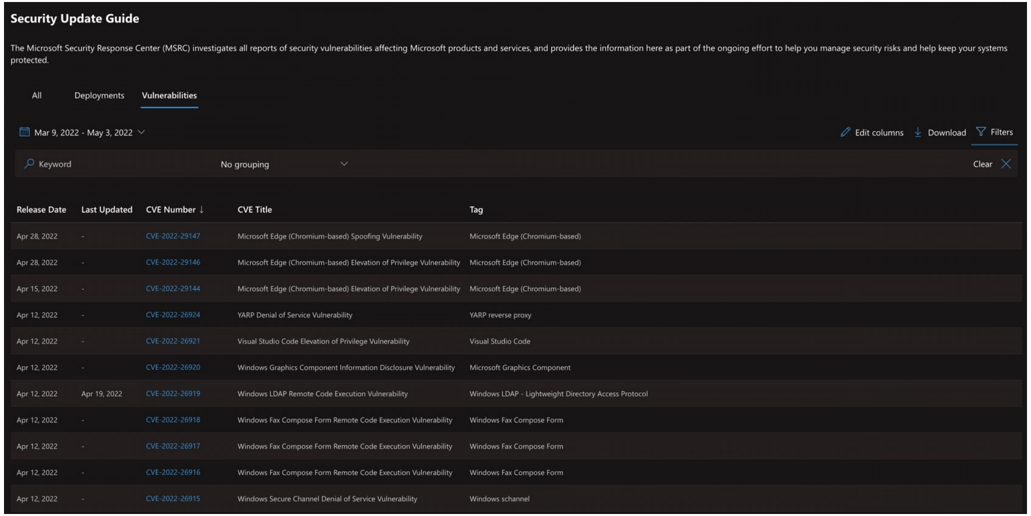
What are the ways that software vulnerabilities are disclosed?



Security Advisories - 2022

Jan 18, 2022

Advisory Number	CVE ID	Release Date	Product	Severity	Link
2022-01	CVE-2021-31821	19 Jan 2022	Octopus Tentacle	Medium	Advisory
2022-02	CVE-2022-23184	7 Feb 2022	Octopus Server	Medium	Advisory



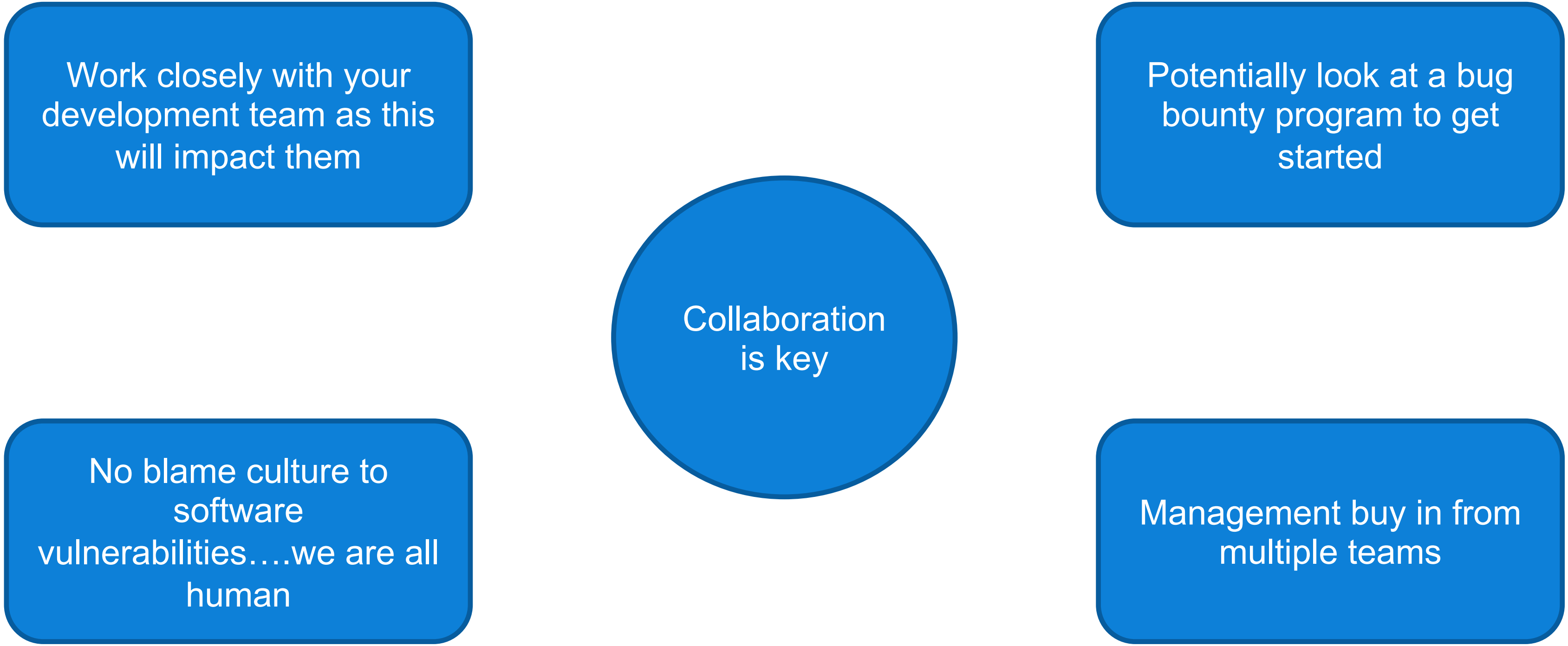
Security Update Guide

The Microsoft Security Response Center (MSRC) investigates all reports of security vulnerabilities affecting Microsoft products and services, and provides the information here as part of the ongoing effort to help you manage security risks and help keep your systems protected.

Release Date	Last Updated	CVE Number ↓	CVE Title	Tag
Apr 28, 2022	-	CVE-2022-29147	Microsoft Edge (Chromium-based) Spoofing Vulnerability	Microsoft Edge (Chromium-based)
Apr 28, 2022	-	CVE-2022-29146	Microsoft Edge (Chromium-based) Elevation of Privilege Vulnerability	Microsoft Edge (Chromium-based)
Apr 15, 2022	-	CVE-2022-29144	Microsoft Edge (Chromium-based) Elevation of Privilege Vulnerability	Microsoft Edge (Chromium-based)
Apr 12, 2022	-	CVE-2022-26924	YARP Denial of Service Vulnerability	YARP reverse proxy
Apr 12, 2022	-	CVE-2022-26921	Visual Studio Code Elevation of Privilege Vulnerability	Visual Studio Code
Apr 12, 2022	-	CVE-2022-26920	Windows Graphics Component Information Disclosure Vulnerability	Microsoft Graphics Component
Apr 12, 2022	Apr 19, 2022	CVE-2022-26919	Windows LDAP Remote Code Execution Vulnerability	Windows LDAP - Lightweight Directory Access Protocol
Apr 12, 2022	-	CVE-2022-26918	Windows Fax Compose Form Remote Code Execution Vulnerability	Windows Fax Compose Form
Apr 12, 2022	-	CVE-2022-26917	Windows Fax Compose Form Remote Code Execution Vulnerability	Windows Fax Compose Form
Apr 12, 2022	-	CVE-2022-26916	Windows Fax Compose Form Remote Code Execution Vulnerability	Windows Fax Compose Form
Apr 12, 2022	-	CVE-2022-26915	Windows Secure Channel Denial of Service Vulnerability	Windows schannel

How do you start disclosing your vulnerabilities?

Changing the business to embrace disclosing vulnerabilities



Work closely with your development team as this will impact them

Potentially look at a bug bounty program to get started

Collaboration is key

No blame culture to software vulnerabilities….we are all human

Management buy in from multiple teams

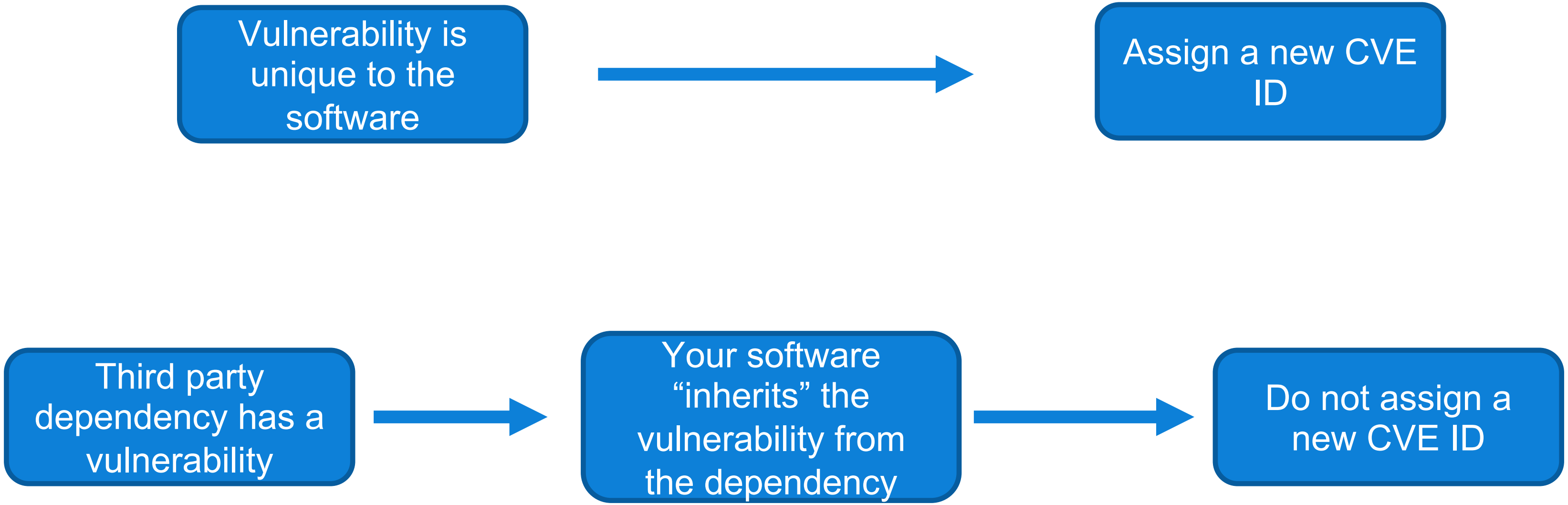
Vulnerability disclosure policy

https://cheatsheetseries.owasp.org/cheatsheets/Vulnerability_Disclosure_Cheat_Sheet.html

What are CVE IDs

CVE = Common Vulnerabilities and Exposures

When to assign CVE IDs



Vulnerability is unique to the software

Assign a new CVE ID

Third party dependency has a vulnerability

Your software “inherits” the vulnerability from the dependency

Do not assign a new CVE ID

What about vulnerabilities in your SaaS platform?

Short answer is no, long answer is maybe

What are the ways you can request a CVE ID?

Non-CNA	CNA
CVE web request	CVE Services
	CVE web request

What is a CVE Numbering Authority (CNA)

Allows certain entities authorized by the CVE program to assign CVE IDs to vulnerabilities and publish CVE records.

Who can be a CNA:

- Software vendors
- Open source maintainers
- Coordination centers
- Bug bounty service providers
- Hosted services
- Research groups

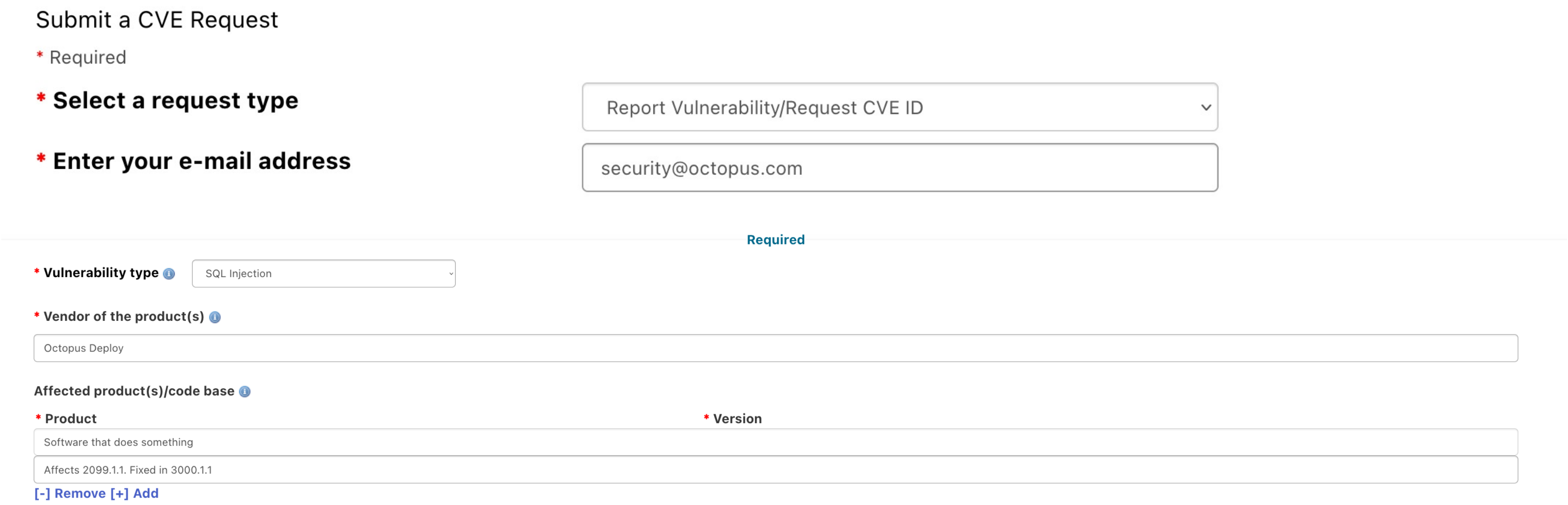
More information about CNAs can be found here: https://www.cve.org/ProgramOrganization/CNAs

Becoming a CVE Numbering Authority (CNA)

Prerequisites:

- Have a public vulnerability disclosure policy
- Have a public source for new vulnerability disclosures

Requesting CVE IDs via Web Request



Submit a CVE Request

* Required

*** Select a request type** Report Vulnerability/Request CVE ID

*** Enter your e-mail address** security@octopus.com

Required

*** Vulnerability type** SQL Injection

*** Vendor of the product(s)**

Octopus Deploy

Affected product(s)/code base

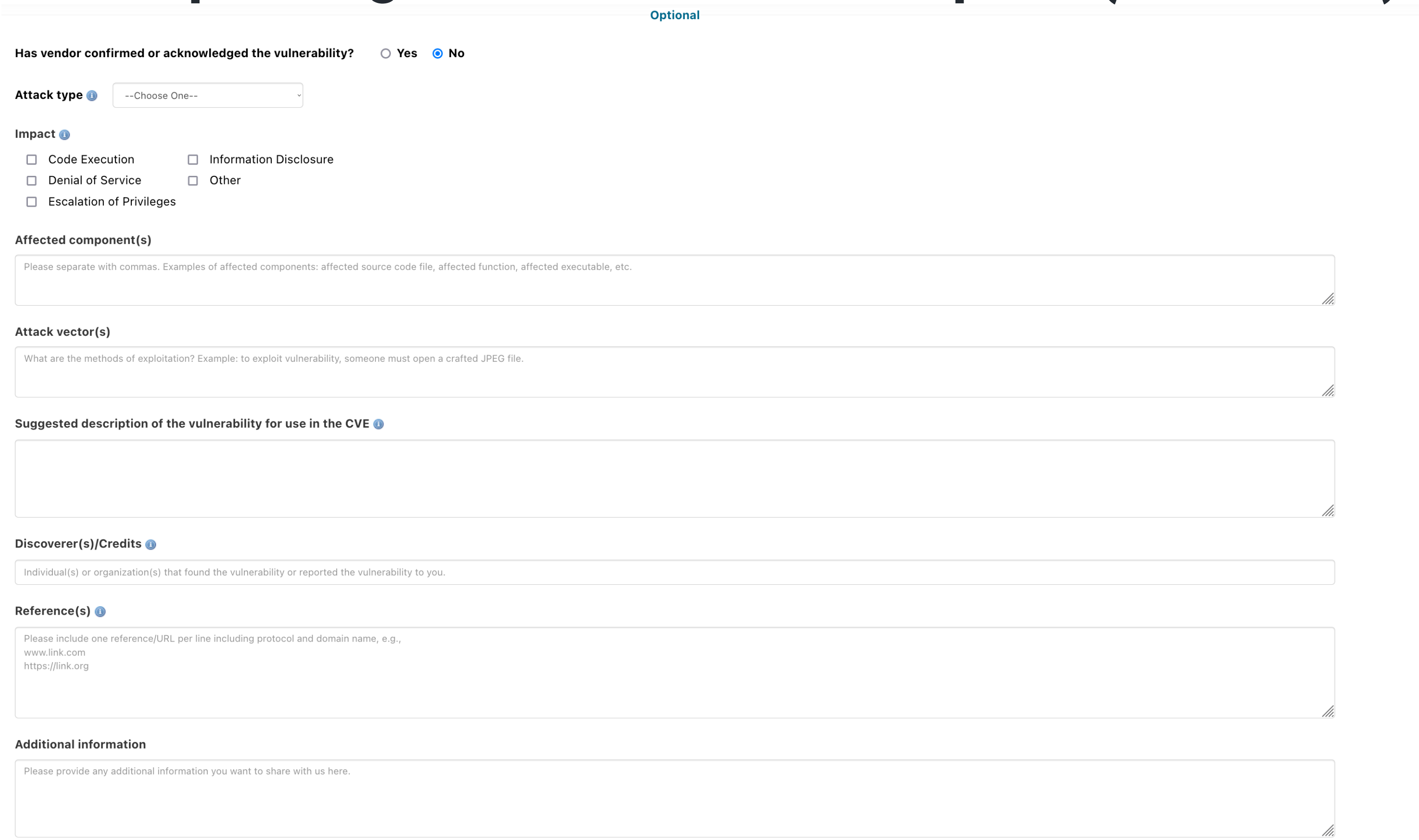
*** Product** *** Version**

Software that does something

Affects 2099.1.1. Fixed in 3000.1.1

[-] Remove [+] Add

Requesting CVE IDs via Web Request (continued)



Optional

Has vendor confirmed or acknowledged the vulnerability? ○ Yes ● No

Attack type --Choose One--

Impact

□ Code Execution
□ Denial of Service
□ Escalation of Privileges
□ Information Disclosure
□ Other

Affected component(s)

Please separate with commas. Examples of affected components: affected source code file, affected function, affected executable, etc.

Attack vector(s)

What are the methods of exploitation? Example: to exploit vulnerability, someone must open a crafted JPEG file.

Suggested description of the vulnerability for use in the CVE

Discoverer(s)/Credits

Individual(s) or organization(s) that found the vulnerability or reported the vulnerability to you.

Reference(s)

Please include one reference/URL per line including protocol and domain name, e.g.,
www.link.com
https://link.org

Additional information

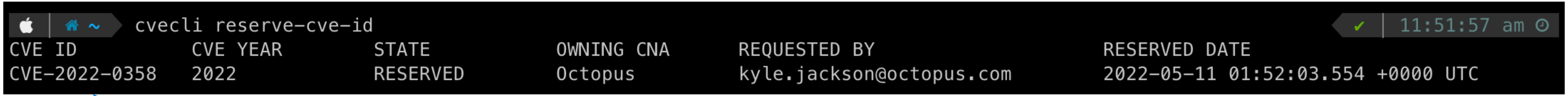
Please provide any additional information you want to share with us here.

Requesting CVE IDs via Web Request (continued)

Pros	Cons
Easy process and doesn’t require anything except a web browser	You don’t get full control over the submission process
	Reviewing requests can take some time so there may be a delay

Requesting CVE IDs programmatically (CNA)

- Allows CNAs to reserve CVE IDs when they are needed
- Does not currently support publishing CVE records (but it is coming)



```
  ~  cvecli reserve-cve-id                                                                                       ✓  11:51:57 am
CVE ID          CVE YEAR        STATE           OWNING CNA      REQUESTED BY                    RESERVED DATE
CVE-2022-0358   2022            RESERVED        Octopus         kyle.jackson@octopus.com        2022-05-11 01:52:03.554 +0000 UTC
```

This is a testing environment we are not Red Hat

Components of a vulnerability disclosure

Vulnerability details

Option 1

SQL Injection in the Events REST API in Octopus Server

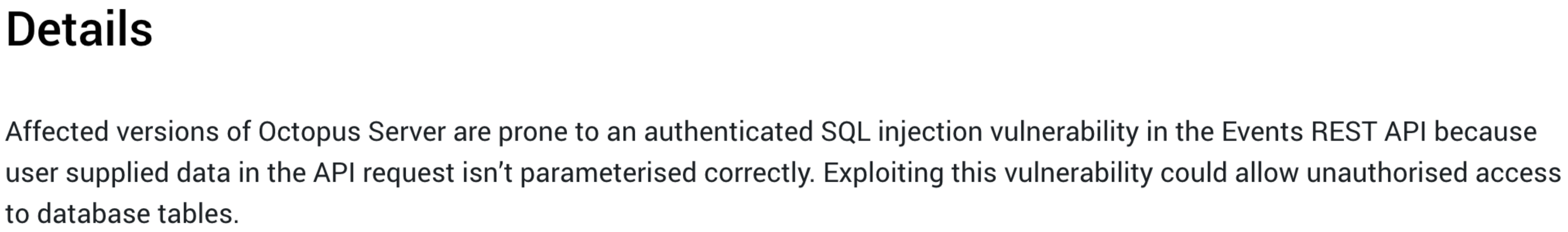
Option 2

Affected versions of Octopus Server are prone to an authenticated SQL injection vulnerability in the Events REST API because user supplied data in the API request isn’t parameterised correctly. Exploiting this vulnerability could allow unauthorised access to database tables.

Option 3

Affected versions of Octopus Server are prone to an authenticated SQL injection vulnerability in the Events REST API. If you supply the following payload <payload> to the API you can retrieve the <table name> table because user supplied data in the API request isn’t parameterised correctly. Exploiting this vulnerability could allow unauthorised access to database tables.

Vulnerability details (continued)



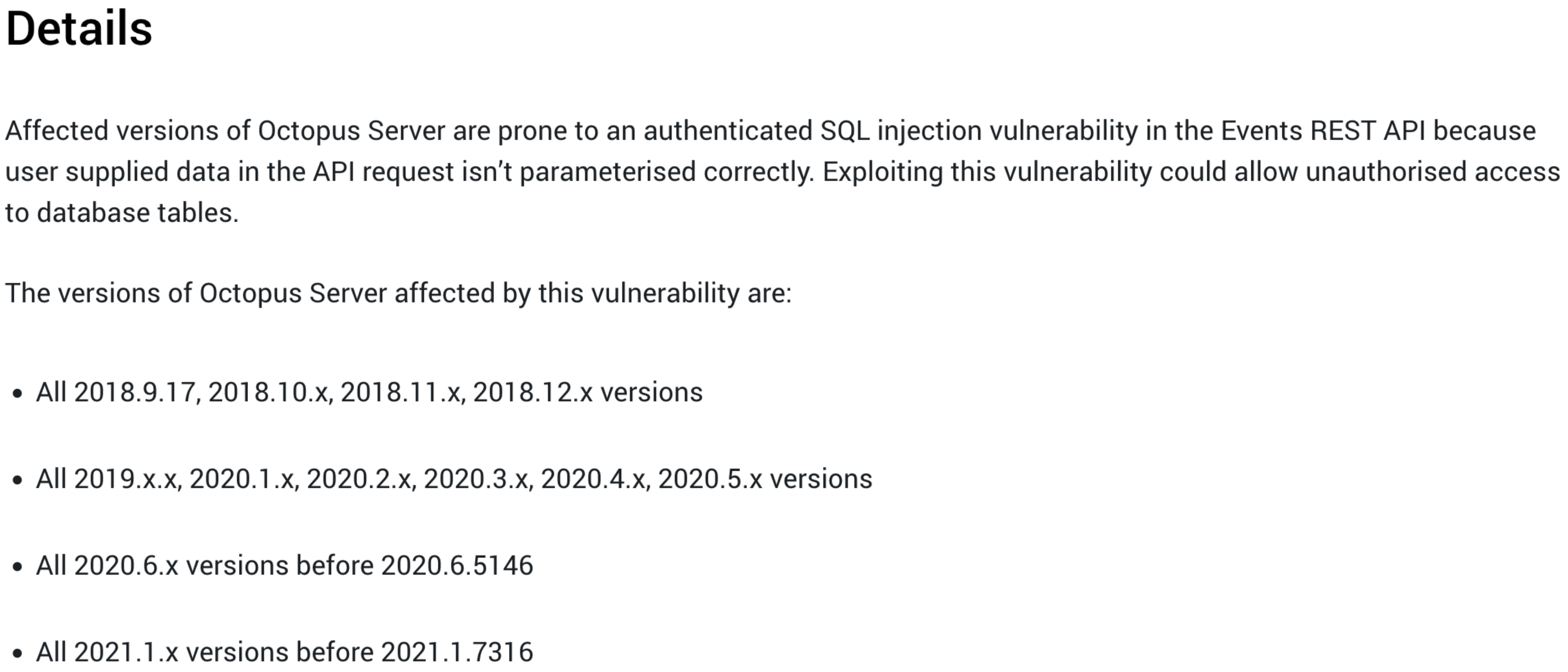
Details

Affected versions of Octopus Server are prone to an authenticated SQL injection vulnerability in the Events REST API because user supplied data in the API request isn’t parameterised correctly. Exploiting this vulnerability could allow unauthorised access to database tables.

Impacted software versions

- What versions of the software product are affected?
- I am on X version do I go to Y version or Z version?

Impacted software versions (continued)



Details

Affected versions of Octopus Server are prone to an authenticated SQL injection vulnerability in the Events REST API because user supplied data in the API request isn't parameterised correctly. Exploiting this vulnerability could allow unauthorised access to database tables.

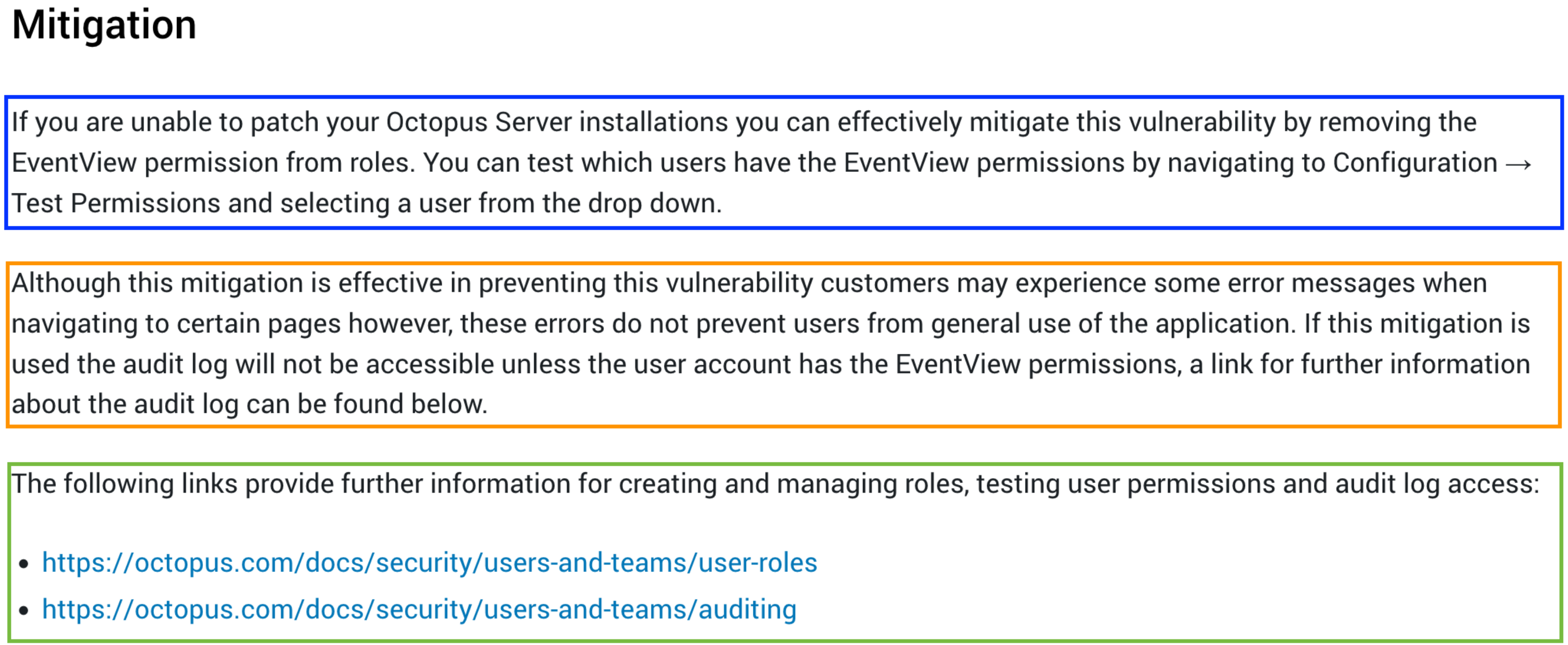
The versions of Octopus Server affected by this vulnerability are:

- All 2018.9.17, 2018.10.x, 2018.11.x, 2018.12.x versions
- All 2019.x.x, 2020.1.x, 2020.2.x, 2020.3.x, 2020.4.x, 2020.5.x versions
- All 2020.6.x versions before 2020.6.5146
- All 2021.1.x versions before 2021.1.7316

Mitigations

- Is there a workaround that can resolve the vulnerability?
- How do you implement the workaround?
- What are the side effects of the workaround?
- Is there any extra information?

Mitigations (continued)



Mitigation

If you are unable to patch your Octopus Server installations you can effectively mitigate this vulnerability by removing the EventView permission from roles. You can test which users have the EventView permissions by navigating to Configuration → Test Permissions and selecting a user from the drop down.

Although this mitigation is effective in preventing this vulnerability customers may experience some error messages when navigating to certain pages however, these errors do not prevent users from general use of the application. If this mitigation is used the audit log will not be accessible unless the user account has the EventView permissions, a link for further information about the audit log can be found below.

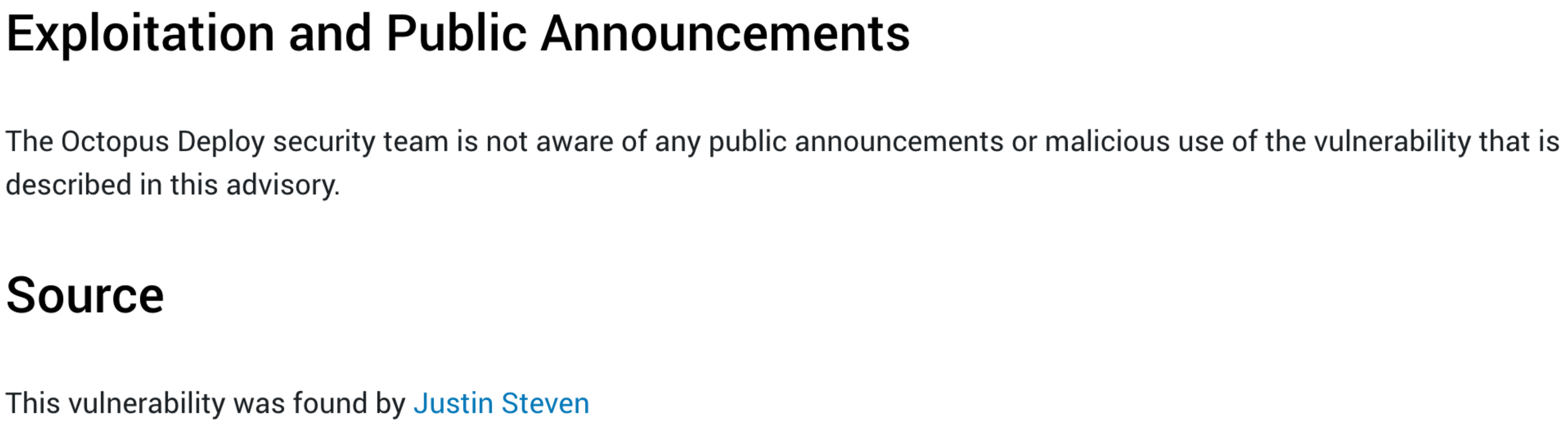
The following links provide further information for creating and managing roles, testing user permissions and audit log access:

- https://octopus.com/docs/security/users-and-teams/user-roles
- https://octopus.com/docs/security/users-and-teams/auditing

Exploitations / Public Announcements and Source

1. Has this vulnerability been exploited?
2. Have there been any public announcements for this vulnerability?
3. Who found the vulnerability?

Exploitations / Public Announcements and Source (continued)



Exploitation and Public Announcements

The Octopus Deploy security team is not aware of any public announcements or malicious use of the vulnerability that is described in this advisory.

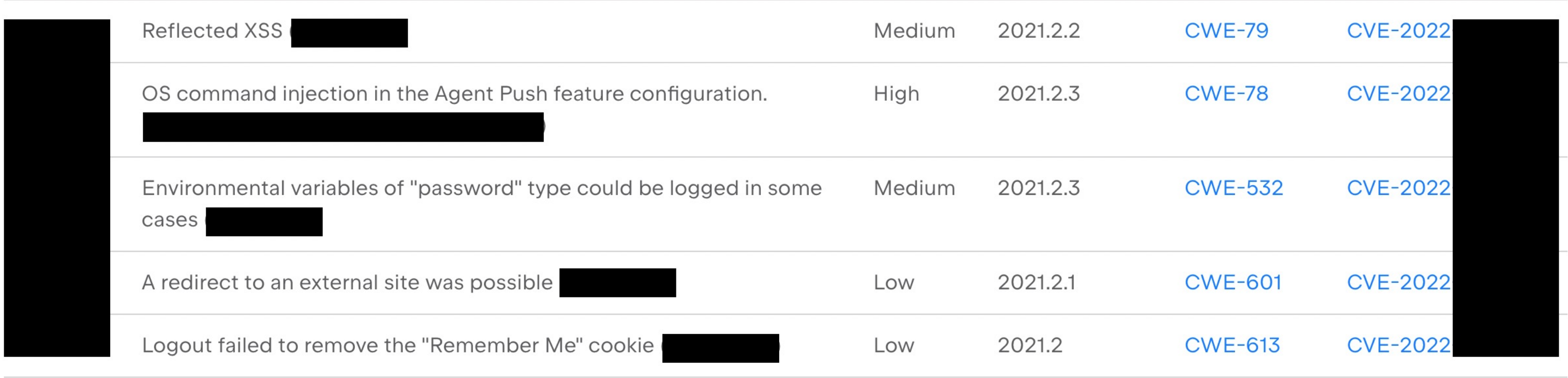
Source

This vulnerability was found by Justin Steven

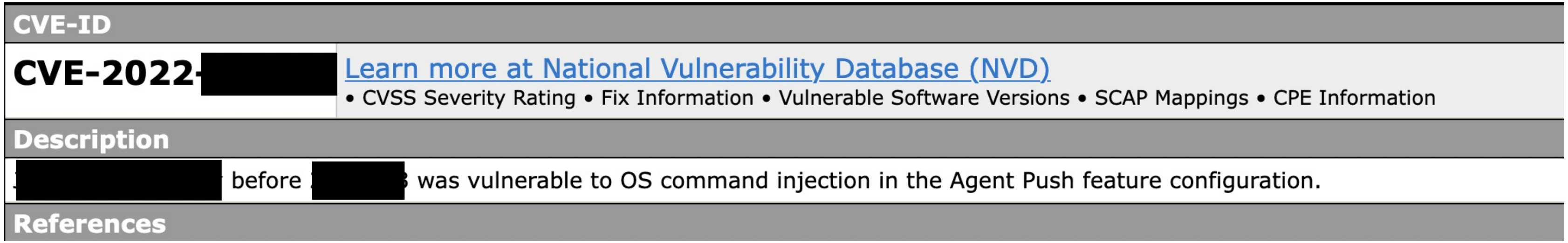
You should end up with something like this…

https://advisories.octopus.com/post/2021/sa2021-04/

You shouldn’t end up with something like this…



[redacted]	Reflected XSS [redacted]	Medium	2021.2.2	CWE-79	CVE-2022[redacted]
[redacted]	OS command injection in the Agent Push feature configuration. [redacted]	High	2021.2.3	CWE-78	CVE-2022[redacted]
[redacted]	Environmental variables of "password" type could be logged in some cases [redacted]	Medium	2021.2.3	CWE-532	CVE-2022[redacted]
[redacted]	A redirect to an external site was possible [redacted]	Low	2021.2.1	CWE-601	CVE-2022[redacted]
[redacted]	Logout failed to remove the "Remember Me" cookie [redacted]	Low	2021.2	CWE-613	CVE-2022[redacted]



CVE-ID

CVE-2022[redacted]

Learn more at National Vulnerability Database (NVD)

• CVSS Severity Rating • Fix Information • Vulnerable Software Versions • SCAP Mappings • CPE Information

Description

[redacted] before [redacted] was vulnerable to OS command injection in the Agent Push feature configuration.

References

Tools that can be used to make publishing vulnerability disclosures easier

Submitting CVE IDs via GitHub (CNA)

When you become a CNA you are provided the process for submitting through the CVE List GitHub Repo

https://github.com/CVEProject/cvelist

Submitting CVE IDs via CVE Services (CNA)

Upcoming feature in the CVE Services API for submitting your CVE records programmatically

Note: You must be a CNA to access this functionality however, if you wanted to try it all the code is public open source so you can run the API locally and try it: https://github.com/CVEProject/cve-services

RSS

Make sure whatever you are using to host your vulnerability disclosures supports RSS

Using Confluence

This can be the easiest approach, you only need two products

Confluence

Scroll Viewport

Using Confluence (continued)

Pros	Cons
You can leverage a Confluence space to “version” all your advisories	Doesn’t support RSS easily out of the box
Doesn’t require web development skills to get working	Doesn’t work well if you want to have an automated process using tooling to reserve CVE IDs
	Can require web development skills to heavily customise
	Requires you to have Confluence and pay for the Scroll Viewport add-on

Static Site Generators

NEXT.JS

Gatsby

HUGO

jekyll

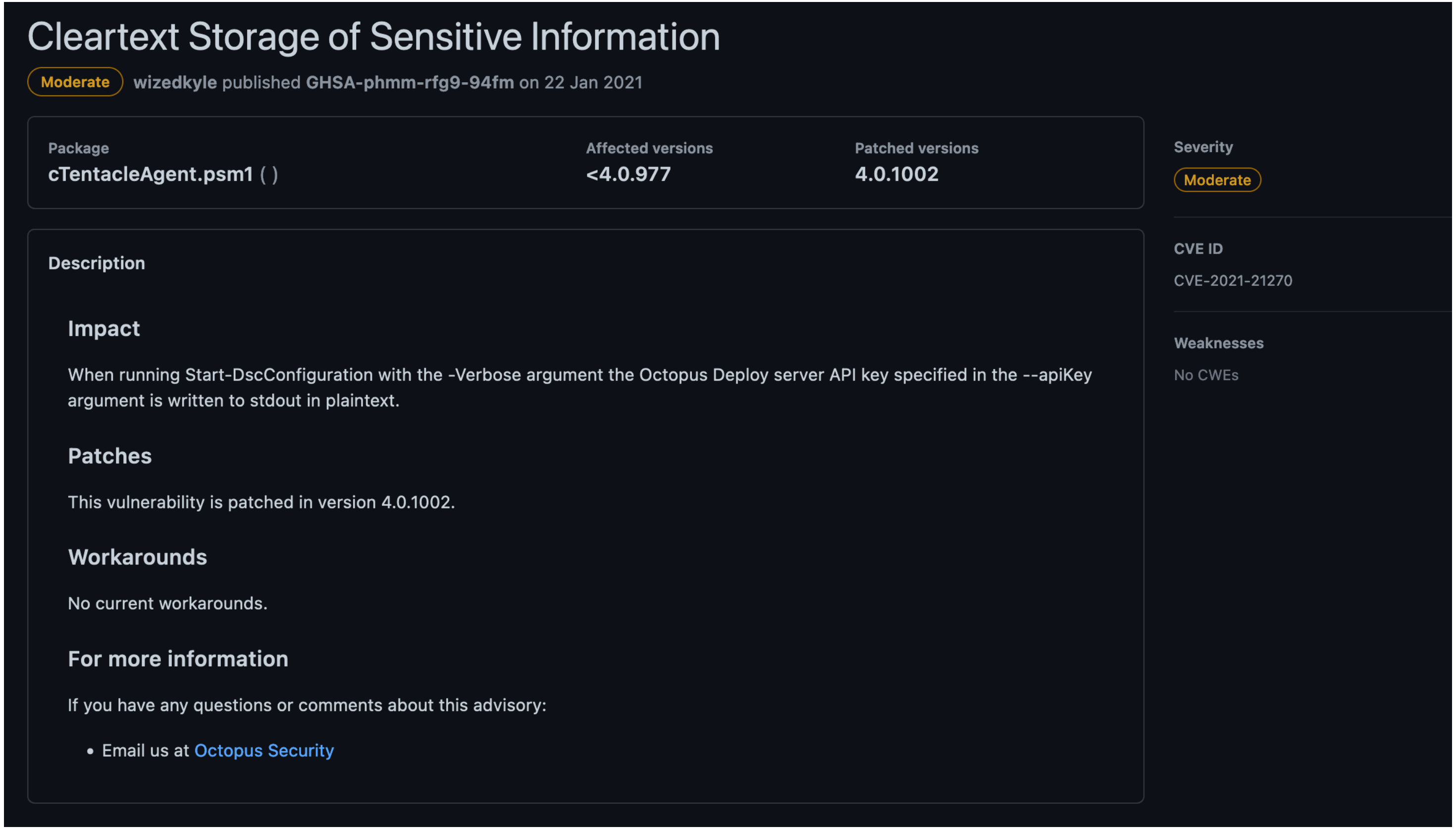
Transform your plain text into static websites and blogs.

There are plenty more to choose from……

Static Site Generators (continued)

Pros	Cons
Generally, support RSS easily out of the box	Requires source control (should hopefully be using it)
Works well if you want to have an automated process using tooling to reserve CVE IDs	You will need to deploy the site and manage any infrastructure you use
Most have theme support so you can easily change the layout of the page	You will have to have some web development skills if you want to change the underlying theme outside of the out of the box customisations
Easily hosted on cloud providers (AWS S3/CloudFront)	

GitHub Security Advisories



Cleartext Storage of Sensitive Information

Moderate **wizedkyle** published **GHSA-phmm-rfg9-94fm** on 22 Jan 2021

Package	Affected versions	Patched versions
cTentacleAgent.psm1 ( )	<4.0.977	4.0.1002

Severity

Moderate

CVE ID

CVE-2021-21270

Weaknesses

No CWEs

Description

Impact

When running Start-DscConfiguration with the -Verbose argument the Octopus Deploy server API key specified in the --apiKey argument is written to stdout in plaintext.

Patches

This vulnerability is patched in version 4.0.1002.

Workarounds

No current workarounds.

For more information

If you have any questions or comments about this advisory:

- Email us at Octopus Security

GitHub Security Advisories (continued)

Pros	Cons
GitHub can assign the CVE IDs for you	You must be using GitHub for your source control
The template is easy to fill out	The repo needs to be public
Integrates nicely into development workflows	

Final Takeaways