detectify

VULNERABILITY REPORT

app.docontrol.io

Scan Started

2021-01-26T21:05:01+00:00

Scan Finished

2021-01-26T23:20:15+00:00

Your findings

Your scan was completed with the following findings discovered.

High	Medium	Low	Information
0	0	0	17

Listed below are your most recent findings, with the most severe listed first. To improve your threat score, prioritise these top issues.

Severity	Issue Type	Times found
INFORMATION	Fingerprinted Software	1
INFORMATION	Amazon S3 Bucket Discovered	1
INFORMATION	Content-Security-Policy / Missing Header	2
INFORMATION	HTML Comments	1
INFORMATION	Missing Content Type	9
INFORMATION	Discovered Host	1
INFORMATION	Crawled URL's	1
INFORMATION	Service Providers	1

1 Fingerprinted Software

Summary

What does this mean?

Invalid fingerprints may cause a audit to take longer, and the lack of fingerprints may cause Detectify to miss running specific tests.

What can happen?

When Detectify audits an application, it collects various fingerprints that indicate what software is running. These fingerprints then allow Detectify to run specific tests when the time is right.

Please make sure Detectify provide accurate data for these fingerprints, by sending us a message in the feedback form on the finding details page.

Found at		CVSS Score
1.1	app.docontrol.io	0

2 Amazon S3 Bucket Discovered

Summary

What does this mean?

No security checks were performed as Detectify was unable to retrieve the bucket name or region. The bucket may or may not still be vulnerable. This finding only indicate that no tests were executed.

What can happen?

Detectify managed to find an Amazon S3 bucket, but failed to decloak it's origin. In order to audit a bucket for security flaws, an attacker must have the bucket name and region.

Found at		CVSS Score
2.1	app.docontrol.io	0

3 Invalid Header Value

Summary

What does this mean?

Browsers may interpret this in different ways, and may open up for undefined behaviors.

What can happen?

The header contain an undefined policy.

Found at		CVSS Score
3.1	http://app.docontrol.io/	0
3.2	http://app.docontrol.io:443/	0

4 HTML Comments

Summary

What does this mean?

The snippets of code within comments will remain inactive until you remove the comment brackets. The comments might also contain sensitive information not meant for the public.

What can happen?

HTML comments, used to store temporary code written by the developers, are visible to the public. Read more at our [https://support.detectify.com/support/solutions/articles/48001048959-html-comments|knowledge base].

Found at		CVSS Score
4.1	https://app.docontrol.io/static/media/login_google_logo.326f60d0.svg	0

5 Missing Content Type

Summary

What does this mean?

It may be possible to conduct XSS attacks against Internet Explorer users, as Internet Explorer recognizes files served with lacking content type as HTML.

What can happen?

The file is being served with a lacking content type header.

Read more [https://support.detectify.com/support/solutions/articles/48001048990-missing-content-type|here].

Found at		CVSS Score
5.1	https://app.docontrol.io/static/media/login_screen.6397d20c.png	0
5.2	https://app.docontrol.io/static/media/login_google_logo.326f60d0.svg	0
5.3	https://app.docontrol.io/	0
5.4	https://app.docontrol.io/static/js/runtime-main.afc3b96a.js	0
5.5	https://app.docontrol.io/static/js/31.84c7355a.chunk.js	0
5.6	https://app.docontrol.io/static/js/main.fd12c4f0.chunk.js	0
5.7	https://app.docontrol.io/static/js/3.98349e1d.chunk.js	0
5.8	https://app.docontrol.io/static/js/10.1b5d154b.chunk.js	0
5.9	https://app.docontrol.io/static/css/10.27506767.chunk.css	0

6 Discovered Host(s)

Summary

What can happen?

Detectify has found the following hosts. This is in no way a vulnerability, but should be considered an indicator for what has been covered.

Read more [https://support.detectify.com/support/solutions/articles/48001048970-discovered-endpoint|here].

Found at		CVSS Score
6.1	app.docontrol.io	0

7 Crawled URL's

Summary

What does this mean?

A scan might take too long due to representative content on the application. Vulnerabilities may also be missed if Detectify lack coverage in some area of the application. If you suspect Detectify can perform better, then take a look at the associated CSV.

What can happen?

This finding is generated for debugging purposes. A link is associated with this finding containing a CSV file with all crawled URL's.

Found at		CVSS Score
7.1	app.docontrol.io	0

8 Service Providers

Summary

What does this mean?

Anyone can retrieve this data. It's only here to serve as an indicator of what vendors have access to.

What can happen?

The listed providers are authorized to host different parts of your infrastructure.

Read more [https://support.detectify.com/support/solutions/articles/48001048980-service-providers|here].

Found at		CVSS Score
8.1	app.docontrol.io	0