detectify

VULNERABILITY REPORT

portal.comensure.com

Scan Started

2021-10-12T12:18:00+00:00

Scan Finished

2021-10-12T14:27:17+00:00

Your findings

Your scan was completed with the following findings discovered.

High	Medium	Low	Information
0	5	0	12

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
MEDIUM	Login over HTTP-GET	1
MEDIUM	Cookie is not set to be HttpOnly	2
MEDIUM	Cookie lack Secure flag	1
MEDIUM	External Links using target='_blank'	1
INFORMATION	Fingerprinted Software	1
INFORMATION	ASP.NET Error Message	3
INFORMATION	Access-Control-Allow-Origin / Invalid Directive	1
INFORMATION	HTML Comments	4
INFORMATION	Discovered Host	1
INFORMATION	Crawled URL's	1
INFORMATION	Service Providers	1

1 Login over HTTP-GET

Summary

What does this mean?

Passwords may appear visible in the URL and stored in the browser's history. It may also be cached by immediate proxies and getting stored in remote server logs.

What can happen?

The login form is sending data using HTTP GET-request.

Found at	CVSS Score
1.1 https://portal.comensure.com/Home/Login/	5

1.1 Login over HTTP-GET

Summary

Found at

https://portal.comensure.com/Home/Login/

CVSS Score

5

Request URL

https://portal.comensure.com/Home/Login/

Request Headers

GET /Home/Login/ HTTP/1.1

Accept	text/html,application/xhtml+xml,application/xml; q=0.9,image/webp,*/*; q=0.8
Upgrade-Insecure-Requests	1
User-Agent	Mozilla/5.0 (compatible; Detectify) +https://detectify.com/bot/aba7f2d6943512ed8fa1898f9475c2b3dbe269a9
Sec-Fetch-Dest	document
Sec-Fetch-Site	same-origin
Sec-Fetch-User	?1
Accept-Encoding	gzip, deflate, br
Accept-Language	en-US
Sec-Fetch-Mode	navigate

Response Headers

HTTP/1.1 200 OK

Server	Microsoft-IIS/10.0
Access-Control-Allow-Origin	http://localhost http://localhost:59779 http://23.99.140.10/ http://23.99.140.10/trusted
Access-Control-Allow-Methods	GET,POST,PUT,DELETE,OPTIONS
Connection	keep-alive
Date	Tue, 12 Oct 2021 12:49:12 GMT
X-AspNetMvc-Version	5.2
Cache-Control	private, s-maxage=0

Access-Control-Allow-Credentials	true
Content-Security-Policy	frame-src http://23.99.140.10 http://23.99.140.10/trusted https://tableau.comensure.com http://tableau.comensure.com http://localhost:59779 https://style1.comensure.com/ http://style1.comensure.com/ https://*.tableau.com; worker-src https://*.comensure.com http://*.comensure.com blob:
X-AspNet-Version	4.0.30319
Content-Length	233650
Content-Security-Policy-Report-Only	frame-src http://localhost http://localhost:59779 http://23.99.140.10 http://23.99.140.10/trusted https://tableau.comensure.com https://style1.comensure.com/ http://style1.comensure.com/ https://*.tableau.com http://tableau.comensure.com; worker-src 'self' http://localhost:* http://*.comensure.com https://*.comensure.com data: gap: blob:; script-src http://23.99.140.10 http://23.99.140.10 'self' http://localhost:* http://*.comensure.com https://*.comensure.com https://*.tableau.com 'unsafe-inline' 'unsafe-eval'
Content-Type	text/html; charset=utf-8
X-Powered-By	ASP.NET

2 Cookie is not set to be HttpOnly

Summary

What does this mean?

If an attacker discovers an XSS he may use it to steal cookies which haven't got the HttpOnly-flag.

What can happen?

One or more cookies lack the HttpOnly flag.

Read more at
[https://support.detectify.com/support/solutions/articles/48001048952-missing-httponly-flag-on-cookies|our knowledge base].

Found at		CVSS Score
2.1	portal.comensure.com	4.3
2.2	portal.comensure.com	4.3

2.1 Cookie is not set to be HttpOnly

Summary

Found at

portal.comensure.com

CVSS Score

4.3

Vulnerable Cookie

ApplicationGatewayAffinity

Cookie

Name	ApplicationGatewayAffinity
Value	2f0302523fbb62ebce3be04a0f58edff
Domain	portal.comensure.com
Path	/
Secure	No
HttpOnly	No
Expires	session

References

DETECTIFY - Detectify Support Center - Missing HttpOnly flag on cookies	https://support.detectify.com/support/solutions/articles/48001048952-missing-httponly-flag-on-cookies
DETECTIFY - What is Security Misconfiguration?	https://www.youtube.com/watch?v=WQ4svQu0Rn8

2.2 Cookie is not set to be HttpOnly

Summary

Found at

portal.comensure.com

CVSS Score

4.3

Vulnerable Cookie

ApplicationGatewayAffinityCORS

Cookie

Name	ApplicationGatewayAffinityCORS
Value	2f0302523fbb62ebce3be04a0f58edff
Domain	portal.comensure.com
Path	/
Secure	Yes
HttpOnly	No
Expires	session

References

DETECTIFY - Detectify Support Center - Missing HttpOnly flag on cookies	https://support.detectify.com/support/solutions/articles/48001048952-missing-httponly-flag-on-cookies
DETECTIFY - What is Security Misconfiguration?	https://www.youtube.com/watch?v=WQ4svQu0Rn8

3 Cookie lack Secure flag

Summary

What does this mean?

On successful exploitation of session cookies, the attacker will be able to set the cookies in his own browser and gain the same privileges as the attacked user. The impact for none-session based cookies varies between systems.

What can happen?

The cookie(s) lack the Secure-flag attribute. An attacker can force the cookie(s) to be sent over plain text HTTP, and can therefor intercept the content.

Read more [https://support.detectify.com/support/solutions/articles/48001048982-cookie-lack-secure-flag|here].

Found at		CVSS Score
3.1	portal.comensure.com	4.1

3.1 Cookie lack Secure flag

Summary

Found at

portal.comensure.com

CVSS Score

4.1

Vulnerable Cookie

ApplicationGatewayAffinity

Cookie

Name	ApplicationGatewayAffinity
Value	2f0302523fbb62ebce3be04a0f58edff
Domain	portal.comensure.com
Path	/
Secure	No
HttpOnly	No
Expires	session

References

OWASP - SecureFlag	https://www.owasp.org/index.php/SecureFlag
PORTSWIGGER - SSL cookie without secure flag set	https://portswigger.net/KnowledgeBase/issues/Details/00500200_SSLcookiewithoutsecureflagset
MISC - Securing Cookies with HttpOnly and secure Flags	http://resources.infosecinstitute.com/securing-cookies-httponly-secure-flags/

4 External Links using target='_blank'

Summary

What does this mean?

The linked page will be able to interact with the originating tab, reading the tab's current URL and redirecting the user to other domains. The linked page will have access to the tab for as long as it remains open.

What can happen?

Links using target='_blank' gain partial access to the linking page via the window.opener object.

Read more
[https://support.detectify.com/support/solutions/articles/48001048981-external-links-using-target-blank-|here].

Found at		CVSS Score
4.1	https://portal.comensure.com/Home/Login/	3.1

4.1 External Links using target='_blank'

Summary

Found at

https://portal.comensure.com/Home/Login/

CVSS Score

3.1

Request URL

https://portal.comensure.com/Home/Login/

Request Headers

GET /Home/Login/ HTTP/1.1

Accept	text/html,application/xhtml+xml,application/xml; q=0.9,image/webp,*/*; q=0.8
Upgrade-Insecure-Requests	1
User-Agent	Mozilla/5.0 (compatible; Detectify) +https://detectify.com/bot/aba7f2d6943512ed8fa1898f9475c2b3dbe269a9
Sec-Fetch-Dest	document
Sec-Fetch-Site	same-origin
Sec-Fetch-User	?1
Accept-Encoding	gzip, deflate, br
Accept-Language	en-US
Sec-Fetch-Mode	navigate

Response Headers

HTTP/1.1 200 OK

Server	Microsoft-IIS/10.0
Access-Control-Allow-Origin	http://localhost http://localhost:59779 http://23.99.140.10/ http://23.99.140.10/trusted
Access-Control-Allow-Methods	GET,POST,PUT,DELETE,OPTIONS
Connection	keep-alive
Date	Tue, 12 Oct 2021 12:49:12 GMT
X-AspNetMvc-Version	5.2
Cache-Control	private, s-maxage=0

Access-Control-Allow-Credentials	true
Content-Security-Policy	frame-src http://23.99.140.10 http://23.99.140.10/trusted https://tableau.comensure.com http://tableau.comensure.com http://localhost:59779 https://style1.comensure.com/ http://style1.comensure.com/ https://*.tableau.com; worker-src https://*.comensure.com http://*.comensure.com blob:
X-AspNet-Version	4.0.30319
Content-Length	233650
Content-Security-Policy-Report-Only	frame-src http://localhost http://localhost:59779 http://23.99.140.10 http://23.99.140.10/trusted https://tableau.comensure.com https://style1.comensure.com/ http://style1.comensure.com/ https://*.tableau.com http://tableau.comensure.com; worker-src 'self' http://localhost:* http://*.comensure.com https://*.comensure.com data: gap: blob:; script-src http://23.99.140.10 http://23.99.140.10 'self' http://localhost:* http://*.comensure.com https://*.comensure.com https://*.tableau.com 'unsafe-inline' 'unsafe-eval'
Content-Type	text/html; charset=utf-8
X-Powered-By	ASP.NET

References

MISC - Target="_blank" - the most underestimated vulnerability ever	https://medium.com/@jitbit/target-blank-the-most-underestimated-vulnerability-ever-96e328301f4c#.oh7ggu8gn
YCOMBINATOR - Hacker News Discussion	https://news.ycombinator.com/item?id=11631292
GITHUB - Target Blank Vulnerability	https://github.com/chafikhnini/target-blank-vulnerability
MISC - When to use target="_blank"	https://css-tricks.com/use-target_blank/
DETECTIFY - Detectify Support Center - External Links using target='_blank'	https://support.detectify.com/support/solutions/articles/48001048981-external-links-using-target-blank-

This finding is only made if the "href" value is an external URL.

In order to mitigate the issue, add the following attribue to your link(s): rel="noopener noreferrer".

Setting target="_blank" on <a> elements now implicitly provides the same rel behavior as setting rel="noopener" in Google Chrome, Microsoft Edge, Firefox and Safari. Internet Explorer and Opera are still vulnerable.

5 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
5.1	portal.comensure.com	0

5.1 Fingerprinted Software

Summary

Found at	CVSS Score
portal.comensure.com	0

References

DETECTIFY - An intelligent way to look for vulnerabilities	https://blog.detectify.com/2016/01/28/an-intelligent-way-to-look-for-vulnerabilities/
DETECTIFY - What's under the hood	https://detectify.com/technology

Vendor: microsoft
Software: iis
Version: 10.0
Confidence: 100

Vendor: microsoft
Software: .net_framework
Version: 4.0.30319
Confidence: 100

Vendor: microsoft
Software: windows
Confidence: 30

Vendor: microsoft
Software: asp.net
Version: 4.0.30319
Confidence: 100

Software: ispconfig

Confidence: 100

6 ASP.NET Error Message

Summary

What does this mean?

Verbose error messages may leak sensitive information. Error messages may also be the result of flawed code.

What can happen?

There is an error message leaking in the application.

Found at		CVSS Score
6.1	https://portal.comensure.com/Content/images/foo%60%3C%25%22%27%7B$%2A%25%5C	0
6.2	https://portal.comensure.com/Content/foo%60%3C%25%22%27%7B$%2A%25%5C	0
6.3	https://portal.comensure.com/foo%60%3C%25%22%27%7B$%2A%25%5C	0

6.1 ASP.NET Error Message

Summary

Found at

https://portal.comensure.com/Content/images/foo%60%3C%25%22%27%7B$%2A%25%5C

CVSS Score

0

Request URL

https://portal.comensure.com/Content/images/foo%60%3C%25%22%27%7B$%2A%25%5C

Request Headers

GET /Content/images/foo%60%3C%25%22%27%7B$%2A%25%5C HTTP/1.1

Upgrade-Insecure-Requests	1
Sec-Fetch-Dest	document
User-Agent	Mozilla/5.0 (compatible; Detectify) +https://detectify.com/bot/aba7f2d6943512ed8fa1898f9475c2b3dbe269a9
Sec-Fetch-Mode	navigate
Accept	text/html,application/xhtml+xml,application/xml; q=0.9,image/webp,*/*; q=0.8
Sec-Fetch-Site	same-origin
Sec-Fetch-User	?1
Accept-Encoding	gzip, deflate, br
Accept-Language	en-US
Host	portal.comensure.com

Response Headers

HTTP/0.0 400 Bad Request

Content-Length	3798
Connection	keep-alive
Date	Tue, 12 Oct 2021 13:56:55 GMT
Content-Type	text/html; charset=utf-8
Access-Control-Allow-Credentials	true

Set-Cookie	ApplicationGatewayAffinityCORS=c657355de02ba9e252f546fd1fefbc81; Path=/; SameSite=None; Secure, ApplicationGatewayAffinity=c657355de02ba9e252f546fd1fefbc81; Path=/
Cache-Control	private
Access-Control-Allow-Methods	GET,POST,PUT,DELETE,OPTIONS
Server	Microsoft-IIS/10.0
X-Aspnet-Version	4.0.30319
X-Powered-By	ASP.NET
Content-Security-Policy	frame-src http://23.99.140.10 http://23.99.140.10/trusted https://tableau.comensure.com http://tableau.comensure.com http://localhost:59779 https://style1.comensure.com/ http://style1.comensure.com/ https://*.tableau.com; worker-src https://*.comensure.com http://*.comensure.com blob:
Content-Security-Policy-Report-Only	frame-src http://localhost http://localhost:59779 http://23.99.140.10 http://23.99.140.10/trusted https://tableau.comensure.com https://style1.comensure.com/ http://style1.comensure.com/ https://*.tableau.com http://tableau.comensure.com; worker-src 'self' http://localhost:* http://*.comensure.com https://*.comensure.com data: gap: blob:; script-src http://23.99.140.10 http://23.99.140.10 'self' http://localhost:* http://*.comensure.com https://*.comensure.com https://*.tableau.com 'unsafe-inline' 'unsafe-eval'
Access-Control-Allow-Origin	http://localhost http://localhost:59779 http://23.99.140.10/ http://23.99.140.10/trusted

References

OWASP - Improper Error Handling	https://owasp.org/www-community/Improper_Error_Handling
MICROSOFT - ASP.NET Error Handling	https://docs.microsoft.com/en-us/aspnet/web-forms/overview/getting-started/getting-started-with-aspnet-45-web-forms/aspnet-error-handling

6.2 ASP.NET Error Message

Summary

Found at

https://portal.comensure.com/Content/foo%60%3C%25%22%27%7B$%2A%25%5C

CVSS Score

0

Request URL

https://portal.comensure.com/Content/foo%60%3C%25%22%27%7B$%2A%25%5C

Request Headers

GET /Content/foo%60%3C%25%22%27%7B$%2A%25%5C HTTP/1.1

Sec-Fetch-User	?1
Accept	text/html,application/xhtml+xml,application/xml; q=0.9,image/webp,*/*; q=0.8
Sec-Fetch-Mode	navigate
Sec-Fetch-Dest	document
Upgrade-Insecure-Requests	1
User-Agent	Mozilla/5.0 (compatible; Detectify) +https://detectify.com/bot/aba7f2d6943512ed8fa1898f9475c2b3dbe269a9
Sec-Fetch-Site	same-origin
Accept-Language	en-US
Accept-Encoding	gzip, deflate, br
Host	portal.comensure.com

Response Headers

HTTP/0.0 400 Bad Request

Date	Tue, 12 Oct 2021 13:40:42 GMT
Access-Control-Allow-Methods	GET,POST,PUT,DELETE,OPTIONS
Content-Length	3798
Connection	keep-alive
Cache-Control	private
X-Aspnet-Version	4.0.30319

Access-Control-Allow-Origin	http://localhost http://localhost:59779 http://23.99.140.10/ http://23.99.140.10/trusted
Content-Type	text/html; charset=utf-8
Set-Cookie	ApplicationGatewayAffinityCORS=c657355de02ba9e252f546fd1fefbc81; Path=/; SameSite=None; Secure, ApplicationGatewayAffinity=c657355de02ba9e252f546fd1fefbc81; Path=/
Content-Security-Policy-Report-Only	frame-src http://localhost http://localhost:59779 http://23.99.140.10 http://23.99.140.10/trusted https://tableau.comensure.com https://style1.comensure.com/ http://style1.comensure.com/ https://*.tableau.com http://tableau.comensure.com; worker-src 'self' http://localhost:* http://*.comensure.com https://*.comensure.com data: gap: blob:; script-src http://23.99.140.10 http://23.99.140.10 'self' http://localhost:* http://*.comensure.com https://*.comensure.com https://*.tableau.com 'unsafe-inline' 'unsafe-eval'
Access-Control-Allow-Credentials	true
Server	Microsoft-IIS/10.0
X-Powered-By	ASP.NET
Content-Security-Policy	frame-src http://23.99.140.10 http://23.99.140.10/trusted https://tableau.comensure.com http://tableau.comensure.com http://localhost:59779 https://style1.comensure.com/ http://style1.comensure.com/ https://*.tableau.com; worker-src https://*.comensure.com http://*.comensure.com blob:

References

OWASP - Improper Error Handling	https://owasp.org/www-community/Improper_Error_Handling
MICROSOFT - ASP.NET Error Handling	https://docs.microsoft.com/en-us/aspnet/web-forms/overview/getting-started/getting-started-with-aspnet-45-web-forms/aspnet-error-handling

6.3 ASP.NET Error Message

Summary

Found at

https://portal.comensure.com/foo%60%3C%25%22%27%7B$%2A%25%5C

CVSS Score

0

Request URL

https://portal.comensure.com/foo%60%3C%25%22%27%7B$%2A%25%5C

Request Headers

GET /foo%60%3C%25%22%27%7B$%2A%25%5C HTTP/1.1

Accept-Language	en-US
User-Agent	Mozilla/5.0 (compatible; Detectify) +https://detectify.com/bot/aba7f2d6943512ed8fa1898f9475c2b3dbe269a9
Upgrade-Insecure-Requests	1
Sec-Fetch-Site	same-origin
Sec-Fetch-User	?1
Accept-Encoding	gzip, deflate, br
Sec-Fetch-Dest	document
Sec-Fetch-Mode	navigate
Accept	text/html,application/xhtml+xml,application/xml; q=0.9,image/webp,*/*; q=0.8
Host	portal.comensure.com

Response Headers

HTTP/0.0 400 Bad Request

Content-Security-Policy-Report-Only	frame-src http://localhost http://localhost:59779 http://23.99.140.10 http://23.99.140.10/trusted https://tableau.comensure.com https://style1.comensure.com/ http://style1.comensure.com/ https://*.tableau.com http://tableau.comensure.com; worker-src 'self' http://localhost:* http://*.comensure.com https://*.comensure.com data: gap: blob:; script-src http://23.99.140.10 http://23.99.140.10 'self' http://localhost:* http://*.comensure.com https://*.comensure.com https://*.tableau.com 'unsafe-inline' 'unsafe-eval'

X-Aspnet-Version	4.0.30319
X-Powered-By	ASP.NET
Content-Security-Policy	frame-src http://23.99.140.10 http://23.99.140.10/trusted https://tableau.comensure.com http://tableau.comensure.com http://localhost:59779 https://style1.comensure.com/ http://style1.comensure.com/ https://*.tableau.com; worker-src https://*.comensure.com http://*.comensure.com blob:
Connection	keep-alive
Access-Control-Allow-Origin	http://localhost http://localhost:59779 http://23.99.140.10/ http://23.99.140.10/trusted
Set-Cookie	ApplicationGatewayAffinityCORS=2f0302523fbb62ebce3be04a0f58edff; Path=/; SameSite=None; Secure, ApplicationGatewayAffinity=2f0302523fbb62ebce3be04a0f58edff; Path=/
Access-Control-Allow-Methods	GET,POST,PUT,DELETE,OPTIONS
Cache-Control	private
Server	Microsoft-IIS/10.0
Access-Control-Allow-Credentials	true
Date	Tue, 12 Oct 2021 13:11:10 GMT
Content-Type	text/html; charset=utf-8
Content-Length	3798

References

OWASP - Improper Error Handling	https://owasp.org/www-community/Improper_Error_Handling
MICROSOFT - ASP.NET Error Handling	https://docs.microsoft.com/en-us/aspnet/web-forms/overview/getting-started/getting-started-with-aspnet-45-web-forms/aspnet-error-handling

7 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
7.1	https://portal.comensure.com/	0

7.1 Access-Control-Allow-Origin / Invalid Directive

Summary

Found at

https://portal.comensure.com/

CVSS Score

0

Request URL

https://portal.comensure.com/

Request Headers

GET / HTTP/1.1

Origin	https://pentest.detectify.com
Referer	https://pentest.detectify.com/
Accept	text/html,application/xhtml+xml,application/xml; q=0.9,image/webp,*/*; q=0.8
User-Agent	Mozilla/5.0 (compatible; Detectify) +https://detectify.com/bot/aba7f2d6943512ed8fa1898f9475c2b3dbe269a9
Host	portal.comensure.com
Cookie	ApplicationGatewayAffinityCORS=2f0302523fbb62ebce3be04a0f58edff; ApplicationGatewayAffinity=2f0302523fbb62ebce3be04a0f58edff
Cache-Control	no-store, no-cache
Pragma	no-cache
Accept-Encoding	gzip, deflate

Response Headers

HTTP/1.1 302 Found

Connection	keep-alive
X-AspNetMvc-Version	5.2
Content-Security-Policy	frame-src http://23.99.140.10 http://23.99.140.10/trusted https://tableau.comensure.com http://tableau.comensure.com http://localhost:59779 https://style1.comensure.com/ http://style1.comensure.com/ https://*.tableau.com; worker-src https://*.comensure.com http://*.comensure.com blob:

Content-Security-Policy-Report-Only	frame-src http://localhost http://localhost:59779 http://23.99.140.10 http://23.99.140.10/trusted https://tableau.comensure.com https://style1.comensure.com/ http://style1.comensure.com/ https://*.tableau.com http://tableau.comensure.com; worker-src 'self' http://localhost:* http://*.comensure.com https://*.comensure.com data: gap: blob:; script-src http://23.99.140.10 http://23.99.140.10 'self' http://localhost:* http://*.comensure.com https://*.comensure.com https://*.tableau.com 'unsafe-inline' 'unsafe-eval'
Access-Control-Allow-Origin	http://localhost http://localhost:59779 http://23.99.140.10/ http://23.99.140.10/trusted
Access-Control-Allow-Methods	GET,POST,PUT,DELETE,OPTIONS
Access-Control-Allow-Credentials	true
Content-Length	156
Cache-Control	private, s-maxage=0
Content-Type	text/html; charset=utf-8
Date	Tue, 12 Oct 2021 12:51:25 GMT
Location	http://portal.comensure.com/Home/Login/
Server	Microsoft-IIS/10.0
X-AspNet-Version	4.0.30319
X-Powered-By	ASP.NET

References

MOZILLA - Cross-Origin Resource Sharing (CORS)	https://developer.mozilla.org/en-US/docs/Web/HTTP/CORS
MISC - I want to add CORS support to my server	https://enable-cors.org/server.html

8 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
8.1	https://portal.comensure.com/bin/	0
8.2	https://portal.comensure.com/Home/ForgotPassword	0
8.3	https://portal.comensure.com/g,vu=new	0
8.4	https://portal.comensure.com/%3f.jsp	0

8.1 HTML Comments

Summary

Found at

https://portal.comensure.com/bin/

CVSS Score

0

Request URL

https://portal.comensure.com/bin/

References

DETECTIFY - Detectify Support Center - HTML Comments	https://support.detectify.com/support/solutions/articles/48001048959-html-comments

8.2 HTML Comments

Summary

Found at

https://portal.comensure.com/Home/ForgotPassword

CVSS Score

0

Request URL

https://portal.comensure.com/Home/ForgotPassword

References

DETECTIFY - Detectify Support Center - HTML Comments	https://support.detectify.com/support/solutions/articles/48001048959-html-comments

8.3 HTML Comments

Summary

Found at

https://portal.comensure.com/g,vu=new

CVSS Score

0

Request URL

https://portal.comensure.com/g,vu=new

References

DETECTIFY - Detectify Support Center - HTML Comments	https://support.detectify.com/support/solutions/articles/48001048959-html-comments

8.4 HTML Comments

Summary

Found at

https://portal.comensure.com/%3f.jsp

CVSS Score

0

Request URL

https://portal.comensure.com/%3f.jsp

References

DETECTIFY - Detectify Support Center - HTML Comments	https://support.detectify.com/support/solutions/articles/48001048959-html-comments

9 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
9.1	portal.comensure.com	0

9.1 Discovered Host

Summary

Found at

portal.comensure.com

CVSS Score

0

Detectify found and tried to access 1 domain, and have analyzed it for security flaws.

portal.comensure.com:
> 20.37.132.37
80/tcp http open
443/tcp https open
443/tcp http open
81/tcp closed
444/tcp closed
2181/tcp closed
2375/tcp closed
2376/tcp closed
3000/tcp closed
3001/tcp closed
3128/tcp closed
3790/tcp closed
4443/tcp closed
4444/tcp closed
4567/tcp closed
4848/tcp closed
5432/tcp closed
5858/tcp closed
5984/tcp closed
5985/tcp closed
5986/tcp closed
6443/tcp closed
7001/tcp closed
7077/tcp closed
8000/tcp closed

8001/tcp closed
8009/tcp closed
8047/tcp closed
8069/tcp closed
8080/tcp closed
8081/tcp closed
8083/tcp closed
8088/tcp closed
8089/tcp closed
8100/tcp closed
8181/tcp closed
8443/tcp closed
8444/tcp closed
8500/tcp closed
8880/tcp closed
8888/tcp closed
9000/tcp closed
9001/tcp closed
9002/tcp closed
9080/tcp closed
9090/tcp closed
9418/tcp closed
9443/tcp closed
11211/tcp closed
16686/tcp closed
50000/tcp closed
50013/tcp closed
50014/tcp closed

10 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
10.1	portal.comensure.com	0

10.1 Crawled URL's

Summary

Found at

portal.comensure.com

CVSS Score

0

References

DETECTIFY - Download Crawled URL's CSV	https://s3-eu-west-1.amazonaws.com/dtfy.crawl/3927cc84f0c163d20314e5addd2ed737/aba7f2d6943512ed8fa1898f9475c2b3dbe269a9/790952ae-d228-4253-aa32-f18ce4b6745d/portal.comensure.com-20211012125O-crawl.csv

Detectify tried to access 57 URL's, 18 of these were identified as unique during crawling and went through further testing.

11 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
11.1	portal.comensure.com	0

11.1 Service Providers

Summary

Found at

portal.comensure.com

CVSS Score

0

References

DETECTIFY - Detectify Support Center - Service Providers	https://support.detectify.com/support/solutions/articles/48001048980-service-providers

ns33.domaincontrol.com

Microsoft