WAS Web Application Report

Qualys. Enterprise

ZA_WAS_BAU_Monthly Report_Slot6_Batch3

20 Feb 2024

Each targeted web application is listed with the total number of detected vulnerabilities and sensitive content.

Janardhan Reddy Gangireddy
vdafn5ag4

Vodafone Group Services
- Global Tech park
Bangalore, Karnataka 560103
India

Target and Filters

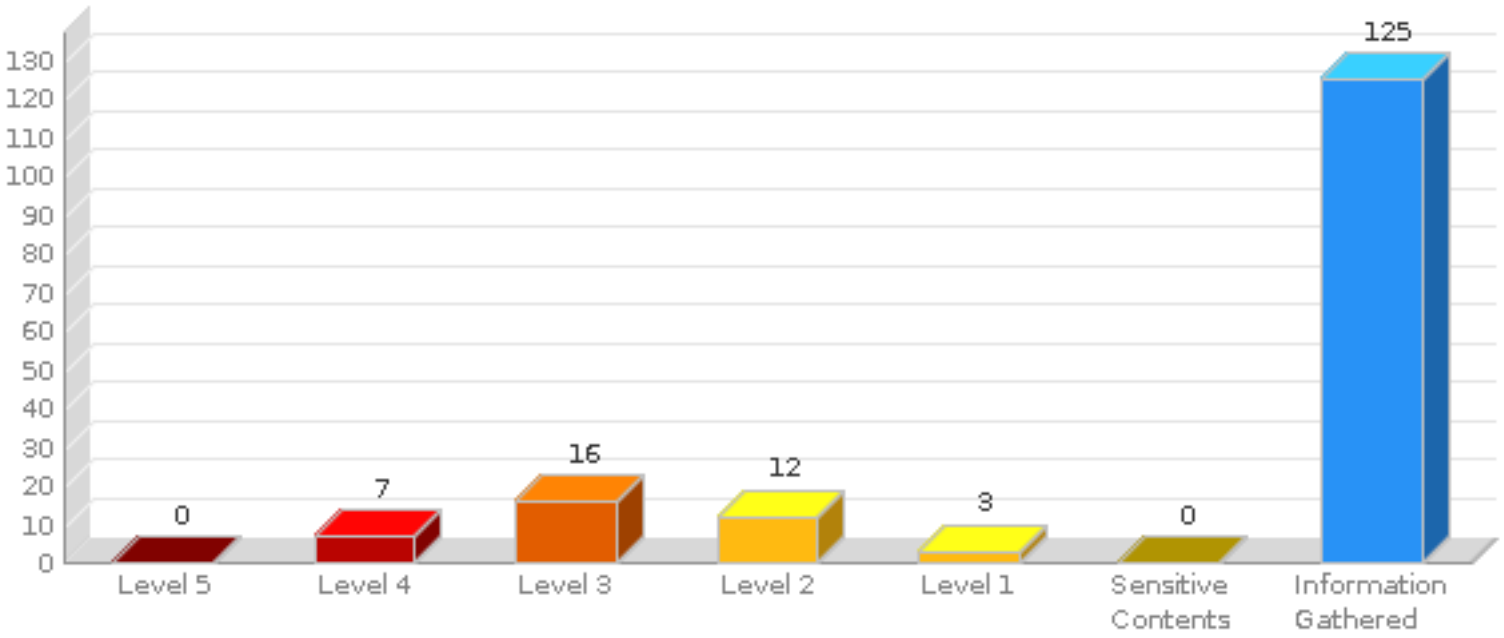
Web Applications (3)	archibus.vodacom.co.za/ archibus.vodacom.co.za/archibus/ archibus.vodacom.co.za:443/fpr/index.asp
Status	New, Active, Re-Opened
Detection Source	Qualys, Burp, Bugcrowd

Summary

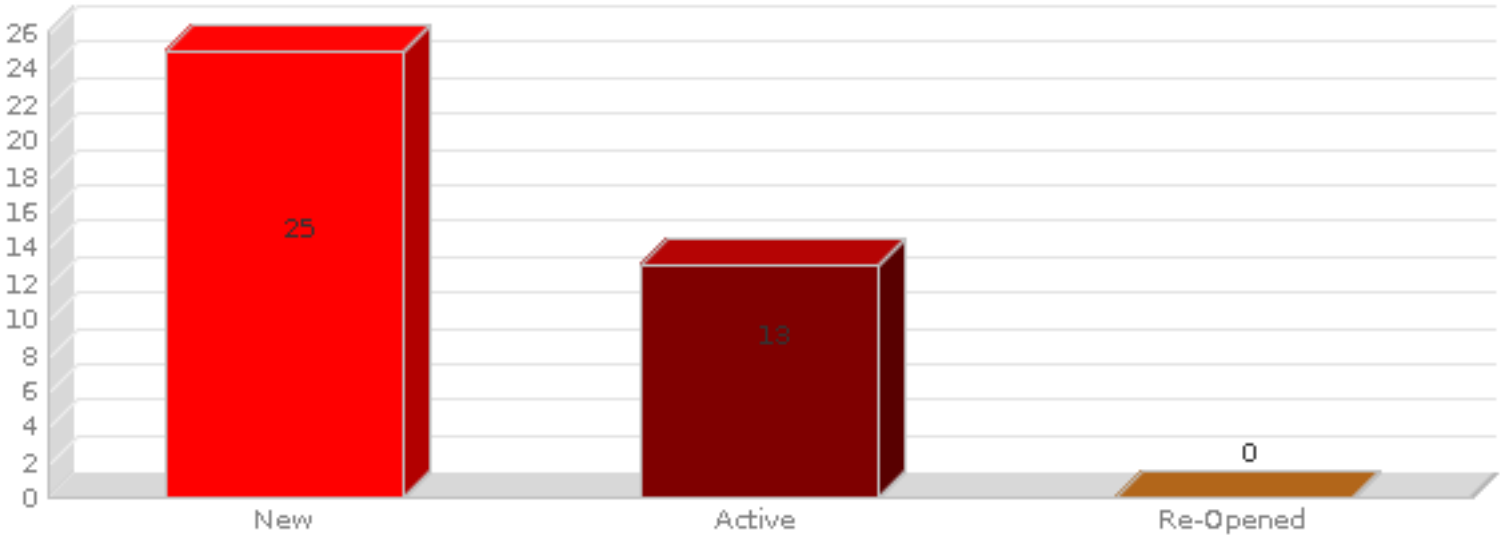
Security Risk	Web Applications	Vulnerabilities	Sensitive Contents	Information Gathered
HIGH	3	38	0	125

WAS Web Application Report

Findings by Severity

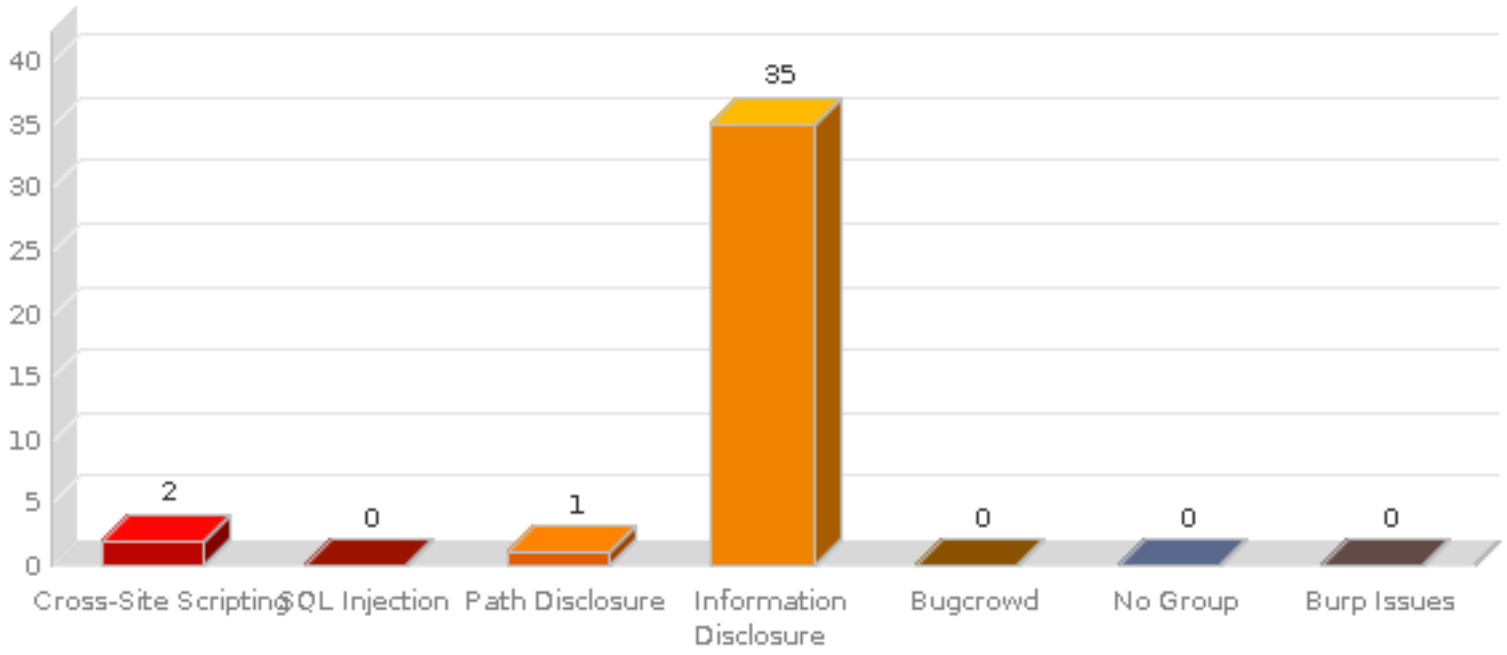


Vulnerabilities by Status

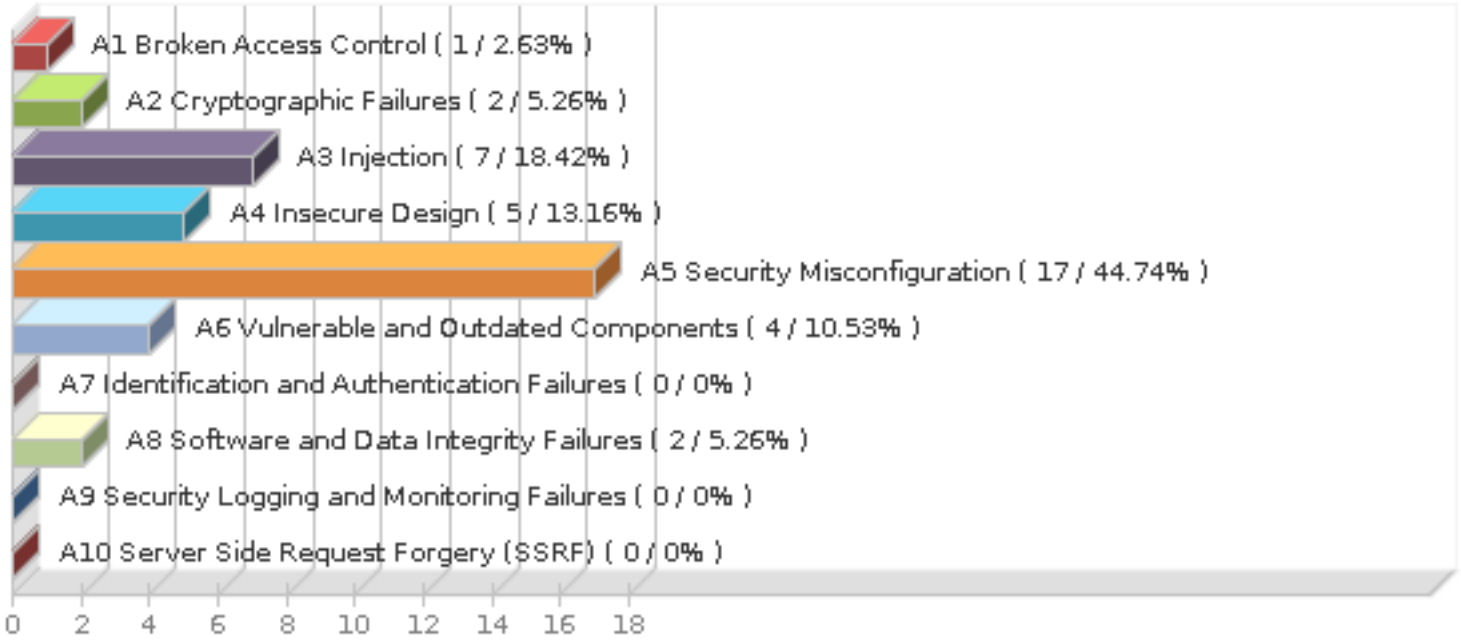


WAS Web Application Report

Vulnerabilities by Group



OWASP Top 10 2021 Vulnerabilities



Web Application	Level 5	Level 4	Level 3	Level 2	Level 1	Sensitive Contents	Information Gathered
archibus.vodacom.co.za/	0	3	6	3	1	0	41
archibus.vodacom.co.za/archibus/	0	3	9	5	1	0	43

WAS Web Application Report

Web Application	Level 5	Level 4	Level 3	Level 2	Level 1	Sensitive Contents	Information Gathered
archibus.vodacom.co.za:443/fpr/index.asp	0	1	1	4	1	0	41

WAS Web Application Report

Results(163)

archibus.vodacom.co.za/ (54)

Vulnerability (13)

Cross-Site Scripting (1)

150541 Apache Tomcat Cross-Site Scripting(XSS) Vulnerability (CVE-2022-34305) (1)

150541 Apache Tomcat Cross-Site Scripting(XSS) Vulnerability (CVE-2022-34305)

archibus.vodacom.co.za/ **New**

URL: https://archibus.vodacom.co.za/LzUc6YsD.1tmhl

Finding #	23855552	**Severity**	Potential Vulnerability - Level 3
Unique #	f736f4a8-3614-4884-b1e3-de24c4b63b8a		
Group	Cross-Site Scripting	**First Time Detected**	11 Feb 2024 21:02 GMT+0200
CWE	CWE-79	**Last Time Detected**	11 Feb 2024 21:02 GMT+0200
OWASP	A3 Injection	**Last Time Tested**	11 Feb 2024 21:02 GMT+0200
WASC	WASC-8 CROSS-SITE SCRIPTING	**Times Detected**	1

CVSS V3 Base	6.1	**CVSS V3 Temporal**	5.3	**CVSS V3 Attack Vector**	Network

Details

Threat

Apache Tomcat is an open source web server and servlet container developed by the Apache Software Foundation.

In affected versions of Apache Tomcat, the Form authentication example in the examples web application displayed user provided data without filtering, exposing a XSS vulnerability.

Affected Versions:
Apache Tomcat 10.1.0-M1 to 10.1.0-M16
Apache Tomcat 10.0.0-M1 to 10.0.22
Apache Tomcat 9.0.30 to 9.0.64
Apache Tomcat 8.5.50 to 8.5.81

QID Detection Logic (Unauthenticated):
This QID sends a HTTP GET request to a invalid URL and based on the response confirms the vulnerable instance of Apache Tomcat running on the host.

Impact

Successful exploitation could allow an attacker to execute arbitrary JavaScript code in the context of the interface or allow the attacker to access sensitive, browser-based information.

Solution

Customers are advised to upgrade Apache Tomcat to new version to remediate this vulnerability. For more information please refer to Apache Tomcat Security Advisory.

Detection Information

Parameter	No param has been required for detecting the information.
Authentication	In order to detect this vulnerability, no authentication has been required.

Payloads

#1 Request

GET https://archibus.vodacom.co.za/LzUc6YsD.1tmhl

Referer: https://archibus.vodacom.co.za/
Cookie: visid_incap_2776849=4d+BhYXLSdeLBPduRDPzlBotyWUAAAAAQUIPAAAAAADu2sh8op936XX+9K7yIEl9;
incap_ses_1687_2776849=cIj9E8eyJWDvLRUgvG1pFxotyWUAAAAAcbKKwG1lgYUyGdvEbUHBwg==;
Host: archibus.vodacom.co.za
User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/102.0.5005.177 Safari/537.36
Accept: */*

Click this link to try to reproduce the vulnerability using above payload.Note that clicking this link may not lead to visible results, either because the vulnerability requires context to be previously set (authentication, cookies...) or because the exploitation of the vulnerability does not lead to any visible proof.

#1 Response

comment: Apache Tomcat Cross-Site Scripting(XSS) Vulnerability (CVE-2022-34305) found at PORT : 443

he requested resource [/LzUc6YsD.1tmhl] is not available Description The origin server did not find a current representation for the target resource or is not willing to disclose that one exists. <hr class="line" /><h3>Apache Tomcat/9.0.62</h3><script type="text/javascript" src="/_Incapsula_Resource?SWJIYLWA=719d34d31c8e3a6e6fffd425f7e032f3&ns=1&cb=1688046905" async></script></body></html>

* The reflected string on the response webpage indicates that the vulnerability test was successful

Information Disclosure (12)

150531 Apache Tomcat EncryptInterceptor DoS Vulnerability (CVE-2022-29885) (1)

150531 Apache Tomcat EncryptInterceptor DoS Vulnerability (CVE-2022-29885) *archibus.vodacom.co.za/* **New**

URL: https://archibus.vodacom.co.za/Zn9rdtw5.1tmhl

Finding #	23855554	**Severity**	Potential Vulnerability - Level 4
Unique #	c2611c9b-d6bf-432b-ab25-64b11a2ce894		
Group	Information Disclosure	**First Time Detected**	11 Feb 2024 21:02 GMT+0200
CWE	CWE-400	**Last Time Detected**	11 Feb 2024 21:02 GMT+0200
OWASP	A6 Vulnerable and Outdated Components	**Last Time Tested**	11 Feb 2024 21:02 GMT+0200
WASC	WASC-10 DENIAL OF SERVICE	**Times Detected**	1

CVSS V3 Base 7.5 **CVSS V3 Temporal** 6.7 **CVSS V3 Attack Vector** Network

Details

Threat

Apache Tomcat is an open source web server and servlet container developed by the Apache Software Foundation.

In affected versions of Apache Tomcat, the documentation for the EncryptInterceptor incorrectly stated it enabled Tomcat clustering to run over an untrusted network. This was not correct. While the EncryptInterceptor does provide confidentiality and integrity protection, it does not protect against all risks associated with running over any untrusted network, particularly DoS risks.

Affected Versions:
Apache Tomcat 10.1.0-M1 to 10.1.0-M14
Apache Tomcat 10.0.0-M1 to 10.0.20
Apache Tomcat 9.0.13 to 9.0.62
Apache Tomcat 8.5.38 to 8.5.78

QID Detection Logic (Unauthenticated):
This QID sends a HTTP GET request to a invalid URL and based on the response confirms the vulnerable instance of Apache Tomcat running on the host.

Impact

Successful exploitation of the vulnerability can allow an attacker to trigger a DoS via an Uncontrolled Resource Consumption

Solution

Upgrade to the Apache Tomcat to the latest version of Apache Tomcat. Please refer to Apache Tomcat Security Advisory.

Detection Information

Parameter	No param has been required for detecting the information.
Authentication	In order to detect this vulnerability, no authentication has been required.

Payloads

#1 Request

GET https://archibus.vodacom.co.za/Zn9rdtw5.1tmhl

Referer: https://archibus.vodacom.co.za/
Cookie: visid_incap_2776849=8Pfr1oKiSHyvifkRCQbJXBQtyWUAAAAAQUIPAAAAAADuHPhwLEgIvFhliV/fdxJJ; incap_ses_1687_2776849=FMa/P+p3/xWBJRUgvG1pFxQtyWUAAAAAgE2PZJSFNNdLEAluwNNEyA==;
Host: archibus.vodacom.co.za
User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/102.0.5005.177 Safari/537.36
Accept: */*

Click this link to try to reproduce the vulnerability using above payload.Note that clicking this link may not lead to visible results, either because the vulnerability requires context to be previously set (authentication, cookies...) or because the exploitation of the vulnerability does not lead to any visible proof.

#1 Response

comment: Apache Tomcat EncryptInterceptor DoS Vulnerability (CVE-2022-29885) found at PORT : 443

he requested resource [/Zn9rdtw5.1tmhl] is not available Description The origin server did not find a current representation for the target resource or is not willing to disclose that one exists. <hr class="line" /><h3>Apache Tomcat/9.0.62</h3><script type="text/javascript" src="/_Incapsula_Resource?SWJIYLWA=719d34d31c8e3a6e6fffd425f7e032f3&ns=1&cb=2023147576" async></script></body></html>

* The reflected string on the response webpage indicates that the vulnerability test was successful

150590 Apache Tomcat HTTP Request Smuggling Vulnerability (CVE-2022-42252) (1)

150590 Apache Tomcat HTTP Request Smuggling Vulnerability (CVE-2022-42252)

archibus.vodacom.co.za/ **New**

URL: https://archibus.vodacom.co.za/gr6R68gy.1tmhl

Finding #	23855550	**Severity**	Potential Vulnerability - Level 4
Unique #	c1470277-e3d4-4f90-b95c-dfeed8b35b94		
Group	Information Disclosure	**First Time Detected**	11 Feb 2024 21:02 GMT+0200
CWE	CWE-20, CWE-444	**Last Time Detected**	11 Feb 2024 21:02 GMT+0200
OWASP	A4 Insecure Design	**Last Time Tested**	11 Feb 2024 21:02 GMT+0200
WASC	WASC-26 HTTP REQUEST SMUGGLING	**Times Detected**	1

CVSS V3 Base	7.5	**CVSS V3 Temporal**	6.5	**CVSS V3 Attack Vector**	Network

Details

Threat

Apache Tomcat is an open source web server and servlet container developed by the Apache Software Foundation.

If Tomcat was configured to ignore invalid HTTP headers via setting rejectIllegalHeader to false (not the default), Tomcat did not reject a request containing an invalid Content-Length header making a request smuggling attack possible if Tomcat was located behind a reverse proxy that also failed to reject the request with the invalid header.

Affected Versions:
Apache Tomcat 10.1.0-M1 to 10.1.0
Apache Tomcat 10.0.0-M1 to 10.0.26
Apache Tomcat 9.0.0-M1 to 9.0.67
Apache Tomcat 8.5.0 to 8.5.52

QID Detection Logic (Unauthenticated):
This QID sends a HTTP GET request to a invalid URL and based on the response confirms the vulnerable instance of Apache Tomcat running on the host.

Impact
Exploitation of the vulnerability could lead to HTTP request smuggling attack.

Solution
Customers are advised to upgrade Apache Tomcat to new version to remediate this vulnerability. For more information please refer to Apache Tomcat Security Advisory.

Detection Information

Parameter	No param has been required for detecting the information.
Authentication	In order to detect this vulnerability, no authentication has been required.

Payloads

#1 Request

GET https://archibus.vodacom.co.za/gr6R68gy.1tmhl
Referer: https://archibus.vodacom.co.za/
Cookie: visid_incap_2776849=gPA23fPuTFK8bwn2vi2GACItyWUAAAAAQUIPAAAAAACDcsI/KoXCQDBqhXeu3rOS;
incap_ses_1687_2776849=gYctIruMGjbUORUgvG1pFyItyWUAAAAAXnbX7UFlT5rxCkg7V3R53A==;
Host: archibus.vodacom.co.za
User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/102.0.5005.177 Safari/537.36
Accept: */*

Click this link to try to reproduce the vulnerability using above payload.Note that clicking this link may not lead to visible results, either because the vulnerability requires context to be previously set (authentication, cookies...) or because the exploitation of the vulnerability does not lead to any visible proof.

#1 Response

comment: Apache Tomcat HTTP Request Smuggling Vulnerability (CVE-2022-42252) found at PORT : 443

he requested resource [/gr6R68gy.1tmhl] is not available Description The origin server did not find a current representation for the target resource or is not willing to disclose that one exists. <hr class="line" /><h3>Apache Tomcat/9.0.62</h3><script type="text/javascript" src="/_Incapsula_Resource?SWJIYLWA=719d34d31c8e3a6e6fffd425f7e032f3&ns=1&cb=1416046868" async></script></body></html>

* The reflected string on the response webpage indicates that the vulnerability test was successful

150755 Apache Tomcat Request Smuggling Vulnerability (CVE-2023-46589) (1)

150755 Apache Tomcat Request Smuggling Vulnerability (CVE-2023-46589)

archibus.vodacom.co.za/ **New**

URL: https://archibus.vodacom.co.za/1LuP6n74.1tmhl

Finding #	23855540	**Severity**	Potential Vulnerability - Level 4
Unique #	3dbfc647-43bb-4c23-9a51-a5cf8a05ed57		
Group	Information Disclosure	**First Time Detected**	11 Feb 2024 21:02 GMT+0200
CWE	CWE-444	**Last Time Detected**	11 Feb 2024 21:02 GMT+0200
OWASP	A4 Insecure Design	**Last Time Tested**	11 Feb 2024 21:02 GMT+0200
WASC		**Times Detected**	

	WASC-26 HTTP REQUEST SMUGGLING				1
CVSS V3 Base	7.5	**CVSS V3 Temporal**	6.5	**CVSS V3 Attack Vector**	Network

Details

Threat

Apache Tomcat is an open source web server and servlet container developed by the Apache Software Foundation.

Tomcat did not correctly parse HTTP trailer headers. A specially crafted trailer header that exceeded the header size limit could cause Tomcat to treat a single request as multiple requests leading to the possibility of request smuggling when behind a reverse proxy.

Affected Versions:
Apache Tomcat 11.0.0-M1 to 11.0.0-M10
Apache Tomcat 10.1.0-M1 to 10.1.15
Apache Tomcat 9.0.0-M1 to 9.0.82
Apache Tomcat 8.5.0 to 8.5.95

QID Detection Logic (Unauthenticated):
This QID sends a HTTP GET request to a invalid URL and based on the response confirms the vulnerable instance of Apache Tomcat running on the host.

Impact

Exploitation of the vulnerability could lead to HTTP request smuggling attack.

Solution

Customers are advised to upgrade relevant versions of Apache Tomcat:
Apache Tomcat 11.0.0-M11 or later
Apache Tomcat 10.1.16 or later
Apache Tomcat 9.0.83 or later
Apache Tomcat 8.5.96 or later
For more information on this vulnerability please refer Apache Tomcat 8 Security Advisory, Apache Tomcat 9 Security Advisory, Apache Tomcat 10 Security Advisory, Apache Tomcat 11 Security Advisory.

Detection Information

Parameter	No param has been required for detecting the information.
Authentication	In order to detect this vulnerability, no authentication has been required.

Payloads

WAS Web Application Report

#1 Request

GET https://archibus.vodacom.co.za/1LuP6n74.1tmhl

Referer: https://archibus.vodacom.co.za/
Cookie: visid_incap_2776849=jPLM4BZmReW0jBTej8jOSoQuyWUAAAAAQUIPAAAAAADABDoimfdHnv9ZXuixrMXK;
incap_ses_1687_2776849=DpxtGh8xBV25XBcgvG1pF4QuyWUAAAAAaIKDPyLsBlZj8iFI2epR3Q==;
Host: archibus.vodacom.co.za
User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/102.0.5005.177 Safari/537.36
Accept: */*

Click this link to try to reproduce the vulnerability using above payload.Note that clicking this link may not lead to visible results, either because the vulnerability requires context to be previously set (authentication, cookies...) or because the exploitation of the vulnerability does not lead to any visible proof.

#1 Response

comment: Apache Tomcat Request Smuggling Vulnerability (CVE-2023-46589) found at PORT : 443

he requested resource [/1LuP6n74.1tmhl] is not available Description The origin server did not find a current representation for the target resource or is not willing to disclose that one exists. <hr class="line" /><h3>Apache Tomcat/9.0.62</h3><script type="text/javascript" src="/_Incapsula_Resource?SWJIYLWA=719d34d31c8e3a6e6fffd425f7e032f3&ns=1&cb=199396187" async></script></body></html>

* The reflected string on the response webpage indicates that the vulnerability test was successful

150263 Insecure Transport (1)

150263 Insecure Transport

archibus.vodacom.co.za/ **New**

URL: http://archibus.vodacom.co.za/Leasure-the-deed-will-the-clipt-Angely-ands-Banq

Finding #	23855556	**Severity**	Confirmed Vulnerability - Level 3
Unique #	87fab6c8-5985-42ed-9002-06e86b2c586d		
Group	Information Disclosure	**First Time Detected**	11 Feb 2024 21:02 GMT+0200
CWE	CWE-319	**Last Time Detected**	11 Feb 2024 21:02 GMT+0200
OWASP	A2 Cryptographic Failures	**Last Time Tested**	11 Feb 2024 21:02 GMT+0200
WASC	WASC-4 INSUFFICIENT TRANSPORT LAYER PROTECTION	**Times Detected**	1

CVSS V3 Base 7.6 **CVSS V3 Temporal** 6.6 **CVSS V3 Attack Vector** Network

Details

Threat

A link is functional over an insecure, HTTP connection. No redirection to HTTPS occurs. Note that this QID is reported for 200/OK responses as well as 4xx and 5xx responses.

Impact

Data sent over a non-HTTPS connection is unencrypted and vulnerable to network sniffing attacks that can expose sensitive or confidential information. This includes non-secure cookies and other potentially sensitive data contained in HTTP headers. Even if no sensitive data is transmitted, man-in-the-middle (MITM) attacks are possible over non-HTTPS connections. An attacker who exploits MITM can intercept and change the conversation between the client (e.g., web browser, mobile device, etc.) and the server.

More information: Why HTTPS Matters

Solution

Ensure that all links are accessible over HTTPS only. The most secure design is for the application to listen and respond only to encrypted HTTPS requests. Alternatively, if non-HTTPS requests are accepted, the server should redirect these requests to HTTPS using a 301 or 302 response.

It is also strongly recommended to use HTTP Strict Transport Security (HSTS) so that web browsers are instructed to use only HTTPS when making requests to the server. QID 150135 will be reported when links without HSTS are found.

For more information, see the Application section of OWASP's Transport Layer Protection Cheat Sheet.

WAS Web Application Report

Detection Information

Parameter	No param has been required for detecting the information.
Authentication	In order to detect this vulnerability, no authentication has been required.

Payloads

#1 Request

GET http://archibus.vodacom.co.za/Leasure-the-deed-will-the-clipt-Angely-ands-Banq

Referer: https://archibus.vodacom.co.za/
Cookie: visid_incap_2776849=FzwYQrB5SDmrEoE8GapjSPYZyWUAAAAAQUIPAAAAAACKSeVsUKW+PDQEFi62u5/P; nlbi_2776849_2147483392=WoCbbZ/T0xODuuO8ZU49BAAAAAC4rTMSqcwSp5j8m2+NYJTV; nlbi_2776849=2+b7ZdTvP3ssIFAPZU49BAAAAAATg/RB/1C/i+jo3xrjvYzk; incap_ses_1687_2776849=lxYnX5C6qRDb7PgfvG1pF/YZyWUAAAAAg7Eia1/rhUGqMH+aaFiXQA==;
Host: archibus.vodacom.co.za
User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/102.0.5005.177 Safari/537.36
Accept: */*

Click this link to try to reproduce the vulnerability using above payload.Note that clicking this link may not lead to visible results, either because the vulnerability requires context to be previously set (authentication, cookies...) or because the exploitation of the vulnerability does not lead to any visible proof.

#1 Response

HTTP/1.0 200 OK
Etag: "4df2a20d"
Content-Type: text/javascript
Content-Length: 240484
Cache-Control: max-age=43, public
Expires: Sun, 11 Feb 2024 19:04:17 GMT
Date: Sun, 11 Feb 2024 19:03:34 GMT
X-CDN: Imperva
Content-Security-Policy-Report-Only: default-src 'self' 'unsafe-eval' 'unsafe-hashes' 'unsafe-inline' data: blob: ; form-action 'none' data: blob: ; report-uri /csp_report
X-Iinfo: 44-8389391-0 0CNN RT(1707678214938 0) q(0 -1 -1 -1) r(0 -1)

(function(){var Oh="kxNLYwsac3tLowsbe2Jrk3szS3Oqoys7o5MLo5ujwyujY2NLM
+vqKyN7GyuzS6MLc9rbkysjC0OaQxsLo6MLyqNzK0tjG2N7k6NzexoBkToBkyvLC2OCYwsrknHDG3trk3FxawuTO3uTgiujCyuTG5OrQztLqqMze5t7kxtLakOjI0u6kyujq3srs3trK5ure2tyeppSEjLI
qTK6NjSzP6K5Oro8Mro/qiwir6okpaEiq6Q6M7cytjo3MrOwqTK5urSoKTK8sLY4JjCyuSSqp7y5NLK2rZGwsLeXtLI6sLIXN7S6ODS5MbmysjQ6MjS7sroxsrkmNjSzM7c0uTo5p7o/La4/
JBywuTkwqbe4LDK6OTK7OTo5sTq5srswsrYyubq3tr

150628 Apache Tomcat JsonErrorReportValve Injection Vulnerability (CVE-2022-45143) (1)

150628 Apache Tomcat JsonErrorReportValve Injection Vulnerability (CVE-2022-45143)

archibus.vodacom.co.za/ **New**

URL: https://archibus.vodacom.co.za/77QDm2nX.1tmhl

Finding #	23855548	**Severity**	Potential Vulnerability - Level 3
Unique #	a443b93f-9122-4ded-9dbc-56ec63770e9d		
Group	Information Disclosure	**First Time Detected**	11 Feb 2024 21:02 GMT+0200
CWE	CWE-74	**Last Time Detected**	11 Feb 2024 21:02 GMT+0200
OWASP	A3 Injection	**Last Time Tested**	11 Feb 2024 21:02 GMT+0200
WASC	WASC-13 INFORMATION LEAKAGE	**Times Detected**	1

CVSS V3 Base 7.5 **CVSS V3 Temporal** 6.5 **CVSS V3 Attack Vector** Network

Details

Threat

Apache Tomcat is an open source web server and servlet container developed by the Apache Software Foundation.

The JsonErrorReportValve did not escape the type, message or description values. In some circumstances these are constructed from user provided data and it

was therefore possible for users to supply values that invalidated or manipulated the JSON output.

Affected Versions:
Apache Tomcat 10.1.0-M1 to 10.1.1
Apache Tomcat 9.0.40 to 9.0.68
Apache Tomcat 8.5.83

QID Detection Logic (Unauthenticated):
This QID sends a HTTP GET request to a invalid URL and based on the response confirms the vulnerable instance of Apache Tomcat running on the host.

Impact
Successful exploitation of this vulnerability allows an attacker to supply values that invalidated or manipulated the JSON output.

Solution
Customers are advised to upgrade Apache Tomcat to new version to remediate this vulnerability. For more information please refer to Apache Tomcat Security Advisory.

Detection Information

Parameter	No param has been required for detecting the information.
Authentication	In order to detect this vulnerability, no authentication has been required.

Payloads

#1 Request

GET https://archibus.vodacom.co.za/77QDm2nX.1tmhl

Referer: https://archibus.vodacom.co.za/
Cookie: visid_incap_2776849=cklCa+KcQ0CvHZyCn4hAYiMtyWUAAAAAQUIPAAAAAABFrUq0ThjIxcne6jNRA039;
incap_ses_1687_2776849=XvklOMnXnDFoOxUgvG1pFyMtyWUAAAAAXxBB/Rpdi2WfDxiVDobw9g==;
Host: archibus.vodacom.co.za
User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/102.0.5005.177 Safari/537.36
Accept: */*

Click this link to try to reproduce the vulnerability using above payload.Note that clicking this link may not lead to visible results, either because the vulnerability requires context to be previously set (authentication, cookies...) or because the exploitation of the vulnerability does not lead to any visible proof.

#1 Response

comment: Apache Tomcat JsonErrorReportValve Injection Vulnerability (CVE-2022-45143) found at PORT : 443

he requested resource [/77QDm2nX.1tmhl] is not available Description The origin server did not find a current representation for the target resource or is not willing to disclose that one exists. <hr class="line" /><h3>Apache Tomcat/9.0.62</h3><script type="text/javascript" src="/_Incapsula_Resource?SWJIYLWA=719d34d31c8e3a6e6fffd425f7e032f3&ns=1&cb=405987239" async></script></body></html>

* The reflected string on the response webpage indicates that the vulnerability test was successful

150662 Apache Tomcat Information Disclosure Vulnerability (CVE-2023-28708) (1)

150662 Apache Tomcat Information Disclosure Vulnerability (CVE-2023-28708) *archibus.vodacom.co.za/* **New**

URL: https://archibus.vodacom.co.za/pffjO750.1tmhl

Finding #	23855546	**Severity**	Potential Vulnerability - Level 3
Unique #	0b57a23e-cec3-4c8b-93b1-39d2065221b1		
Group	Information Disclosure	**First Time Detected**	11 Feb 2024 21:02 GMT+0200
CWE	CWE-523	**Last Time Detected**	11 Feb 2024 21:02 GMT+0200

WAS Web Application Report

OWASP	A8 Software and Data Integrity Failures	**Last Time Tested**	11 Feb 2024 21:02 GMT+0200
WASC	WASC-13 INFORMATION LEAKAGE	**Times Detected**	1

CVSS V3 Base	4.3	**CVSS V3 Temporal**	3.8	**CVSS V3 Attack Vector**	Network

Details

Threat

Apache Tomcat is an open source web server and servlet container developed by the Apache Software Foundation.

Tomcat's RemoteIpFilter, when used with HTTP requests received from a reverse proxy that includes the X-Forwarded-Proto header set to https, may cause session cookies created by Tomcat to be transmitted over an insecure channel if the secure attribute is not included in the cookies. This could potentially expose sensitive user data to attackers.

Affected Versions:
Apache Tomcat 11.0.0-M1 to 11.0.0-M2
Apache Tomcat 10.1.0-M1 to 10.1.5
Apache Tomcat 9.0.0-M1 to 9.0.71
Apache Tomcat 8.5.0 to 8.5.85

QID Detection Logic (Unauthenticated):
This QID sends a HTTP GET request to a invalid URL and based on the response confirms the vulnerable instance of Apache Tomcat running on the host.

Impact

Insecure transmission of session cookies could potentially expose sensitive user data to attackers.

Solution

To address this vulnerability, it is recommended that customers upgrade to one of the following versions of Apache Tomcat: 11.0.0-M3, 10.1.6, 9.0.72, or 8.5.86, or install a newer version. For additional information, please refer to the Apache Tomcat Security Advisory.

Detection Information

Parameter	No param has been required for detecting the information.
Authentication	In order to detect this vulnerability, no authentication has been required.

Payloads

#1 Request

GET https://archibus.vodacom.co.za/pffjO750.1tmhl

Referer: https://archibus.vodacom.co.za/
Cookie: visid_incap_2776849=Hyp/nvKOS0mAQiGtj24MJVktyWUAAAAAQUIPAAAAAAArOXfgMetCVkdkTiNsryDL;
incap_ses_1687_2776849=B1LjKEYDOVqnjBUgvG1pF1ktyWUAAAAAf9XM1XFuU/9JabYjZGZx9Q==;
Host: archibus.vodacom.co.za
User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/102.0.5005.177 Safari/537.36
Accept: */*

Click this link to try to reproduce the vulnerability using above payload.Note that clicking this link may not lead to visible results, either because the vulnerability requires context to be previously set (authentication, cookies...) or because the exploitation of the vulnerability does not lead to any visible proof.

#1 Response

comment: Apache Tomcat Information Disclosure Vulnerability (CVE-2023-28708) found at PORT : 443

he requested resource [/pffjO750.1tmhl] is not available Description The origin server did not find a current representation for the target resource or is not willing to disclose that one exists. <hr class="line" /><h3>Apache Tomcat/9.0.62</h3><script type="text/javascript" src="/_Incapsula_Resource?
SWJIYLWA=719d34d31c8e3a6e6fffd425f7e032f3&ns=1&cb=351395777" async></script></body></html>

* The reflected string on the response webpage indicates that the vulnerability test was successful

150687 Apache Tomcat FileUpload Denial Of Service (DoS) Vulnerability (CVE-2023-24998) (1)

150687 Apache Tomcat FileUpload Denial Of Service (DoS) Vulnerability (CVE-2023-24998)

archibus.vodacom.co.za/ **New**

URL: https://archibus.vodacom.co.za/sko3dkCB.1tmhl

Finding #	23855544	**Severity**	Potential Vulnerability - Level 3
Unique #	3648ca79-2ce7-4dd7-a7e5-0c2b143fbb80		
Group	Information Disclosure	**First Time Detected**	11 Feb 2024 21:02 GMT+0200
CWE	CWE-770	**Last Time Detected**	11 Feb 2024 21:02 GMT+0200
OWASP	A6 Vulnerable and Outdated Components	**Last Time Tested**	11 Feb 2024 21:02 GMT+0200
WASC	WASC-10 DENIAL OF SERVICE	**Times Detected**	1

CVSS V3 Base 7.5 **CVSS V3 Temporal** 6.7 **CVSS V3 Attack Vector** Network

Details

Threat

Apache Tomcat is an open source web server and servlet container developed by the Apache Software Foundation.

Apache Tomcat uses a packaged renamed copy of Apache Commons FileUpload to provide the file upload functionality defined in the Jakarta Servlet specification. Apache Tomcat was, therefore, also vulnerable to the Apache Commons FileUpload vulnerability CVE-2023-24998 as there was no limit to the number of request parts processed. This resulted in the possibility of an attacker triggering a DoS with a malicious upload or series of uploads.

Affected Products:
Apache Tomcat from version 8.5.0 to 8.5.84
Apache Tomcat from version 9.0.0-M1 to 9.0.70
Apache Tomcat from version 10.1.0-M1 to 10.1.4
Apache Tomcat version 11.0.0-M1

QID Detection Logic (Unauthenticated):
This QID sends a HTTP GET request to a invalid URL and based on the response confirms the vulnerable instance of Apache Tomcat running on the host.

Impact

Successful exploitation of the vulnerability can allow an attacker to trigger a DoS via malicious upload or series of uploads

Solution

Upgrade to the Apache Tomcat to the latest version of Apache Tomcat. Please refer to Apache Tomcat 8 Security, Apache Tomcat 9 Security, Apache Tomcat 10 Security, Apache Tomcat 11 Security.

Detection Information

Parameter	No param has been required for detecting the information.
Authentication	In order to detect this vulnerability, no authentication has been required.

Payloads

#1 Request

GET https://archibus.vodacom.co.za/sko3dkCB.1tmhl

Referer: https://archibus.vodacom.co.za/
Cookie: visid_incap_2776849=1dkepUKgR/OqGUZvc/bXu2otyWUAAAAAQUIPAAAAAADZI48fB3YQvFG2/AhbOeNP;
incap_ses_1687_2776849=rQ8CCXxuZ2xcqBUgvG1pF2otyWUAAAAA3XCCBfrT2a7gVXH9IYPcWQ==;
Host: archibus.vodacom.co.za
User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/102.0.5005.177 Safari/537.36
Accept: */*

Click this link to try to reproduce the vulnerability using above payload.Note that clicking this link may not lead to visible results, either because the vulnerability requires context to be previously set (authentication, cookies...) or because the exploitation of the vulnerability does not lead to any visible proof.

#1 Response

comment: Apache Tomcat FileUpload Denial Of Service (DoS) Vulnerability (CVE-2023-24998) found at PORT: 443

he requested resource [/sko3dkCB.1tmhl] is not available Description The origin server did not find a current representation for the target resource or is not willing to disclose that one exists. <hr class="line" /><h3>Apache Tomcat/9.0.62</h3><script type="text/javascript" src="/_Incapsula_Resource?SWJIYLWA=719d34d31c8e3a6e6fffd425f7e032f3&ns=1&cb=613756321" async></script></body></html>

* The reflected string on the response webpage indicates that the vulnerability test was successful

150704 Apache Tomcat Open Redirect Vulnerability (CVE-2023-41080) (1)

150704 Apache Tomcat Open Redirect Vulnerability (CVE-2023-41080)

archibus.vodacom.co.za/ **New**

URL: https://archibus.vodacom.co.za/z3r1JSyE.1tmhl

Finding #	23855542	**Severity**	Potential Vulnerability - Level 3
Unique #	77666117-17e0-4330-9126-676dc7544dea		
Group	Information Disclosure	**First Time Detected**	11 Feb 2024 21:02 GMT+0200
CWE	CWE-601	**Last Time Detected**	11 Feb 2024 21:02 GMT+0200
OWASP	A3 Injection	**Last Time Tested**	11 Feb 2024 21:02 GMT+0200
WASC	WASC-38 URL REDIRECTOR ABUSE	**Times Detected**	1

CVSS V3 Base	6.1	**CVSS V3 Temporal**	5.3	**CVSS V3 Attack Vector**	Network

Details

Threat

Apache Tomcat is an open source web server and servlet container developed by the Apache Software Foundation.

If the ROOT (default) web application is configured to use FORM authentication then it is possible that a specially crafted URL could be used to trigger a redirect to an URL of the attackers choice.

Affected Versions:
Apache Tomcat 11.0.0-M1 to 11.0.0-M10
Apache Tomcat 10.1.0-M1 to 10.1.12
Apache Tomcat 9.0.0-M1 to 9.0.79
Apache Tomcat 8.5.0 to 8.5.92

QID Detection Logic (Unauthenticated):
This QID sends a HTTP GET request to a invalid URL and based on the response confirms the vulnerable instance of Apache Tomcat running on the host.

Impact
Successful exploitation could allow attackers to trick a user into visiting a specially crafted link which would redirect them to an arbitrary malicious external URL.

Solution
To address this vulnerability, it is recommended that customers upgrade to one of the following versions of Apache Tomcat: 11.0.0-M11, 10.1.13, 9.0.80, or 8.5.93, or install a newer version. For additional information, please refer to the Apache Tomcat Security Advisory.

Detection Information

Parameter	No param has been required for detecting the information.
Authentication	In order to detect this vulnerability, no authentication has been required.

Payloads

#1 Request

GET https://archibus.vodacom.co.za/z3r1JSyE.1tmhl
Referer: https://archibus.vodacom.co.za/
Cookie: visid_incap_2776849=0euXHMlGSI6HJhg5vwPiZ54tyWUAAAAAQUIPAAAAAADxj3oxDkrq5gappRM47EfW; incap_ses_1687_2776849=iRsUVKACARjY+BUgvG1pF54tyWUAAAAAPq0QvpK9so2gvsxPN1Kiqw==;
Host: archibus.vodacom.co.za
User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/102.0.5005.177 Safari/537.36
Accept: */*

Click this link to try to reproduce the vulnerability using above payload.Note that clicking this link may not lead to visible results, either because the vulnerability requires context to be previously set (authentication, cookies...) or because the exploitation of the vulnerability does not lead to any visible proof.

#1 Response

comment: Apache Tomcat Open Redirect Vulnerability (CVE-2023-41080) found at PORT : 443

he requested resource [/z3r1JSyE.1tmhl] is not available Description The origin server did not find a current representation for the target resource or is not willing to disclose that one exists. <hr class="line" /><h3>Apache Tomcat/9.0.62</h3><script type="text/javascript" src="/_Incapsula_Resource?SWJIYLWA=719d34d31c8e3a6e6fffd425f7e032f3&ns=1&cb=1615876560" async></script></body></html>

* The reflected string on the response webpage indicates that the vulnerability test was successful

150122 Cookie Does Not Contain The "secure" Attribute (1)

150122 Cookie Does Not Contain The "secure" Attribute — *archibus.vodacom.co.za/* **Active**

URL: https://archibus.vodacom.co.za/

Finding #	18387172	**Severity**	Confirmed Vulnerability - Level 2
Unique #	648d43e0-22b5-4014-8e0f-f8df585d14ba		
Group	Information Disclosure	**First Time Detected**	22 Jan 2023 21:57 GMT+0200
CWE	CWE-614	**Last Time Detected**	11 Feb 2024 21:02 GMT+0200
OWASP	A5 Security Misconfiguration	**Last Time Tested**	11 Feb 2024 21:02 GMT+0200
WASC		**Times Detected**	

	WASC-4 INSUFFICIENT TRANSPORT LAYER PROTECTION				15
CVSS V3 Base	4.3	CVSS V3 Temporal	4.1	CVSS V3 Attack Vector	Network

Details

Threat
The cookie does not contain the "secure" attribute.

Impact
Cookies with the "secure" attribute are only permitted to be sent via HTTPS. Cookies sent via HTTP expose an unsuspecting user to sniffing attacks that could lead to user impersonation or compromise of the application account.

Solution
If the associated risk of a compromised account is high, apply the "secure" attribute to cookies and force all sensitive requests to be sent via HTTPS.

Detection Information

Cookie Name(s)	**visid_incap_2776849, incap_ses_1687_2776849, nlbi_2776849, nlbi_2776849_2147483392**
Authentication	In order to detect this vulnerability, no authentication has been required.

Payloads

#1 Request

GET https://archibus.vodacom.co.za/

Host: archibus.vodacom.co.za
User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/102.0.5005.177 Safari/537.36
Accept: */*

Click this link to try to reproduce the vulnerability using above payload.Note that clicking this link may not lead to visible results, either because the vulnerability requires context to be previously set (authentication, cookies...) or because the exploitation of the vulnerability does not lead to any visible proof.

#1 Response

visid_incap_2776849=FzwYQrB5SDmrEoE8GapjSPYZyWUAAAAAQUIPAAAAAACKSeVsUKW+PDQEFi62u5/P; expires=Sun Feb 9 22:21:11 2025; path=/; domain=.vodacom.co.za; max-age=31459842; httponly
Cookies set via JavaScript do not have an associated HTTP response header.

incap_ses_1687_2776849=lxYnX5C6qRDb7PgfvG1pF/YZyWUAAAAg7Eia1/rhUGqMH+aaFiXQA==; path=/; domain=.vodacom.co.za
Cookies set via JavaScript do not have an associated HTTP response header.

nlbi_2776849=2+b7ZdTvP3ssIFAPZU49BAAAAAATg/RB/1C/i+jo3xrjvYzk; path=/; domain=.vodacom.co.za
Cookies set via JavaScript do not have an associated HTTP response header.

nlbi_2776849_2147483392=WoCbbZ/T0xODuuO8ZU49BAAAAAC4rTMSqcwSp5j8m2+NYJTV; path=/; domain=.vodacom.co.za
Cookies set via JavaScript do not have an associated HTTP response header.

150123 Cookie Does Not Contain The "HTTPOnly" Attribute (1)

150123 Cookie Does Not Contain The "HTTPOnly" Attribute

archibus.vodacom.co.za/ **Active**

URL: https://archibus.vodacom.co.za/

Finding #	18387174	**Severity**	Confirmed Vulnerability - Level 2
Unique #	3e094e9a-a462-4516-9861-6886b2cdff22		
Group	Information Disclosure	**First Time Detected**	22 Jan 2023 21:57 GMT+0200
CWE	CWE-1004	**Last Time Detected**	11 Feb 2024 21:02 GMT+0200
OWASP	A5 Security Misconfiguration	**Last Time Tested**	11 Feb 2024 21:02 GMT+0200
WASC	WASC-4 INSUFFICIENT TRANSPORT LAYER PROTECTION	**Times Detected**	15

CVSS V3 Base	4.3	CVSS V3 Temporal	4.1	CVSS V3 Attack Vector	Network

Details

Threat
The cookie does not contain the "HTTPOnly" attribute.

Impact
Cookies without the "HTTPOnly" attribute are permitted to be accessed via JavaScript. Cross-site scripting attacks can steal cookies which could lead to user impersonation or compromise of the application account.

Solution
If the associated risk of a compromised account is high, apply the "HTTPOnly" attribute to cookies.

Detection Information

Cookie Name(s)	**nlbi_2776849_2147483392, incap_ses_1687_2776849, nlbi_2776849**
Authentication	In order to detect this vulnerability, no authentication has been required.

Payloads

#1 Request

GET https://archibus.vodacom.co.za/

Host: archibus.vodacom.co.za
User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/102.0.5005.177 Safari/537.36
Accept: */*

Click this link to try to reproduce the vulnerability using above payload.Note that clicking this link may not lead to visible results, either because the vulnerability requires context to be previously set (authentication, cookies...) or because the exploitation of the vulnerability does not lead to any visible proof.

#1 Response

nlbi_2776849_2147483392=WoCbbZ/T0xODuuO8ZU49BAAAAAC4rTMSqcwSp5j8m2+NYJTV; path=/; domain=.vodacom.co.za
Cookies set via JavaScript do not have an associated HTTP response header.

incap_ses_1687_2776849=lxYnX5C6qRDb7PgfvG1pF/YZyWUAAAAAg7Eia1/rhUGqMH+aaFiXQA==; path=/; domain=.vodacom.co.za
Cookies set via JavaScript do not have an associated HTTP response header.

nlbi_2776849=2+b7ZdTvP3ssIFAPZU49BAAAAAATg/RB/1C/i+jo3xrjvYzk; path=/; domain=.vodacom.co.za
Cookies set via JavaScript do not have an associated HTTP response header.

150476 Cookies Issued Without User Consent (1)

150476 Cookies Issued Without User Consent

archibus.vodacom.co.za/ **Active**

URL: https://archibus.vodacom.co.za/

Finding #	18387170	**Severity**	Confirmed Vulnerability - Level 2
Unique #	ebfd0b26-d972-4c28-b70b-99c603cffaea		
Group	Information Disclosure	**First Time Detected**	22 Jan 2023 21:57 GMT+0200
CWE	CWE-565	**Last Time Detected**	11 Feb 2024 21:02 GMT+0200
OWASP	A5 Security Misconfiguration	**Last Time Tested**	11 Feb 2024 21:02 GMT+0200
WASC	-	**Times Detected**	15

CVSS V3 Base	5.3	CVSS V3 Temporal	4.5	CVSS V3 Attack Vector	Network

WAS Web Application Report

Details

Threat
The cookies listed in the Results section were issued from the web application during the crawl without accepting any opt-in dialogs.

Impact
Cookies may be set without user explicitly agreeing to accept them.

Solution
Review the application to ensure that all cookies listed are supposed to be issued without user opt-in. If the EU Cookie law is applicable for this web application, ensure these cookies require user opt-in or have been classified as exempt by your organization.

Detection Information

Parameter	No param has been required for detecting the information.
Authentication	In order to detect this vulnerability, no authentication has been required.

Payloads

#1 Request

GET https://archibus.vodacom.co.za/

Host: archibus.vodacom.co.za
User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/102.0.5005.177 Safari/537.36
Accept: */*

Click this link to try to reproduce the vulnerability using above payload.Note that clicking this link may not lead to visible results, either because the vulnerability requires context to be previously set (authentication, cookies...) or because the exploitation of the vulnerability does not lead to any visible proof.

#1 Response

Total cookies: 4
visid_incap_2776849=MIK5RtFxTUOpWe6NawPwYqYryWUAAAAAQUIPAAAAAABT//PYhsA3YMLNnGEdhceL; HttpOnly; expires=Sun, 09-Feb-2025 22:21:11 GMT; domain=.vodacom.co.za; path=/ First set at URL: https://archibus.vodacom.co.za/_Incapsula_Resource?SWJIYLWA=719d34d31c8e3a6e6fffd425f7e032f3&ns=89&cb=463486056
incap_ses_1687_2776849=J+goctug1Ti/8BIgvG1pF6YryWUAAAAAD2sQ21kFBTclQDjS4qFH0w==; domain=.vodacom.co.za; path=/ First set at URL: https://archibus.vodacom.co.za/_Incapsula_Resource?SWJIYLWA=719d34d31c8e3a6e6fffd425f7e032f3&ns=89&cb=463486056
nlbi_2776849=QtxDDBFRtmwvC0UxZU49BAAAAABXwhmoQooaqGjGo2ZsW35Q; domain=.vodacom.co.za; path=/ First set at URL: https://archibus.vodacom.co.za/_Incapsula_Resource?SWJIYLWA=719d34d31c8e3a6e6fffd425f7e032f3&ns=89&cb=463486056
nlbi_2776849_2147483392=dFZ8eRx8rAmYvS8tZU49BAAAAADRi1LwTRC23ZXAgaJ3iwEv; domain=.vodacom.co.za; path=/ First set at URL: https://archibus.vodacom.co.za/_Incapsula_Resource?SWJIYLWA=719d34d31c8e3a6e6fffd425f7e032f3&ns=89&cb=463486056

150630 CORS header misconfigured (1)

150630 CORS header misconfigured

archibus.vodacom.co.za/ **Active**

URL: https://archibus.vodacom.co.za/Leasure-the-deed-will-the-clipt-Angely-ands-Banq?d=archibus.vodacom.co.za

Finding #	19067696	**Severity**	Potential Vulnerability - Level 1
Unique #	0782fd92-f63f-44fb-9d2d-db25f9ac078e		
Group	Information Disclosure	**First Time Detected**	18 Mar 2023 01:17 GMT+0200
CWE	CWE-942	**Last Time Detected**	11 Feb 2024 21:02 GMT+0200
OWASP	A5 Security Misconfiguration	**Last Time Tested**	11 Feb 2024 21:02 GMT+0200
WASC	-	**Times Detected**	13

CVSS V3 Base	4.3	**CVSS V3 Temporal**	4	**CVSS V3 Attack Vector**	Network

Details

WAS Web Application Report

Threat

Cross-Origin Resource Sharing (CORS) is an HTTP-header based mechanism that allows a server to indicate any origins (domain, scheme, or port) other than its own from which a browser should permit loading resources. CORS also relies on a mechanism by which browsers make a "preflight" request to the server hosting the cross-origin resource, in order to check that the server will permit the actual request. In that preflight, the browser sends headers that indicate the HTTP method and headers that will be used in the actual request. For security reasons, browsers restrict cross-origin HTTP requests initiated from scripts. The "Access-Control-Allow-Origin" header is used to specify the allowed origins to access the resource.

The WAS scanning engine detects the vulnerability by examining the "Access-Control-Allow-Origin" header for a wildcard value (*). This value in the response to an XHR request indicate that the resource can be accessed from any domain and needs to be strictly configured.

Impact

If CORS is misconfigured, it can lead to major security risk like access to sensitive data, API keys and other users' data from any domain. This access could lead to misuse and exploitation of protected resource.

Solution

CORS header misconfiguration can be addressed by providing only the list of allowed domains in the "Access-Control-Allow-Origin" header. The wildcard character (*) should never be provided as it indicates any domain can access the resource.

Detection Information

Parameter	No param has been required for detecting the information.
Authentication	In order to detect this vulnerability, no authentication has been required.
Access Path	Here is the path followed by the scanner to reach the exploitable URL:

https://archibus.vodacom.co.za/

Payloads

#1 Request

POST https://archibus.vodacom.co.za/Leasure-the-deed-will-the-clipt-Angely-ands-Banq? d=archibus.vodacom.co.za

Origin: http://azbycxdwev.com
Referer: https://archibus.vodacom.co.za/
Cookie: visid_incap_2776849=FzwYQrB5SDmrEoE8GapjSPYZyWUAAAAAQUIPAAAAAACKSeVsUKW+PDQEFi62u5/P; nlbi_2776849_2147483392=w2zdKHwQ2BkXRE6CZU49BAAAAADbxZE3z4288nxmMYLmUSzY; nlbi_2776849=2+b7ZdTvP3ssIFAPZU49BAAAAAATg/RB/1C/i+jo3xrjvYzk; incap_ses_1687_2776849=lxYnX5C6qRDb7PgfvG1pF/YZyWUAAAAAg7Eia1/rhUGqMH+aaFiXQA==;
Host: archibus.vodacom.co.za
User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/102.0.5005.177 Safari/537.36
Accept: */*
Content-Type: application/x-www-form-urlencoded

-

Click this link to try to reproduce the vulnerability using above payload.Note that clicking this link may not lead to visible results, either because the vulnerability requires context to be previously set (authentication, cookies...) or because the exploitation of the vulnerability does not lead to any visible proof.

#1 Response

comment: CORS header Access-Control-Allow-Origin is misconfigured or is too permissive.

Response headers:
access-control-allow-origin: *
server-timing: bon, total;dur=0.047438
server: bon
connection: keep-alive
keep-alive: timeout=60
content-length: 0
date: Sun, 11 Feb 2024 19:52:36 GMT
Set-Cookie: nlbi_2776849_2147483392=VnPfKeQk4RGlaofXZU49BAAAAAAKN9Rtb3A0uxBF91zg8942; path=/; Domain=.vodacom.co.za
Set-Cookie: incap_ses_1687_2776849=tAGpTsG3kzMvdAcgvG1pF4QlyWUAAAAAy31vFMy6kKZfx2IMsGmgUA==; path=/; Domain=.vodacom.co.za
X-CDN: Imperva
Content-Security-Policy-Report-Only: default-src 'self' 'unsafe-eval' 'unsafe-hashes' 'unsafe-inline' data: blob: ; form-action 'none' data: blob: ; report-uri /csp_report
X-Iinfo: 0-11139783-11139784 NNNN CT(9 9 0) RT(1707681155974 2) q(0 0 0 0) r(1 1) U6

WAS Web Application Report

Information Gathered (41)

Information Gathered (1)

150497 Progressive scan completely crawled and tested the website (1)

150497 Progressive scan completely crawled and tested the website

archibus.vodacom.co.za

Finding #	10974667	**Severity**	Information Gathered - Level 1
Unique #	011c9848-31b0-4e65-8445-a4ea1a0cfedf		
Group	Information Gathered		
CWE	-	**Detection Date**	11 Feb 2024 21:02 GMT+0200
OWASP	-		
WASC	-		

Details

Threat

Scan covered the whole scope of the web application and finished all test phases.
QID is reported, starting from progression 2. When progression 1 is launched and scan is finished it is considered as single scan, hence QID will not be reported.
If subsequent scans are completed with all phases QID 150497 will be reported.

Impact

N/A

Solution

Review QID 150021 for additional details of phases completed during this scan.

Results

Scan covered the whole scope of the web application and finished all test phases.

Scan Diagnostics (26)

150018 Connection Error Occurred During Web Application Scan (1)

150018 Connection Error Occurred During Web Application Scan

archibus.vodacom.co.za

Finding #	10540454	**Severity**	Information Gathered - Level 2
Unique #	8728dfae-2b2e-4f11-9b49-2f8d2bce9458		
Group	Scan Diagnostics		
CWE	-	**Detection Date**	11 Feb 2024 21:02 GMT+0200
OWASP	-		
WASC	-		

Details

Threat

The following are some of the possible reasons for the timeouts or connection errors:
1. A disturbance in network connectivity between the scanner and the web application occurred.
2. The web server or application server hosting the application was taken down in the midst of a scan.
3. The web application experienced an overload, possibly due to load generated by the scan.
4. An error occurred in the SSL/TLS handshake (applies to HTTPS web applications only).
5. A security device, such as an IDS/IPS or web application firewall (WAF), began to drop or reject the HTTP connections from the scanner.
6. Very large files like PDFs, videos, etc. are present on the site and caused timeouts when accessed by the scanner.

Impact

Some of the links were not crawled or scanned. Results may be incomplete or incorrect.

Solution

First, confirm that the server was not taken down in the midst of the scan. After that, investigate the root cause by reviewing the listed links and examining web server logs, application server logs, or IDS/IPS/WAF logs. If the errors are caused due to load generated by the scanner then try reducing the scan intensity (this could increase the scan duration). If the errors are due to specific URLs being tested by the scanner or due to specific form data sent by the scanner, then configure exclude lists in the scan configuration as needed to avoid such requests. If timeouts or connection errors are a persistent issue but you want the scan to run to completion, change the Behavior Settings in the option profile to increase the error thresholds or disable the error checks entirely.

Results

Total number of unique links that encountered timeout errors: 87
Links with highest number of timeouts:
14 https://archibus.vodacom.co.za/
9 https://archibus.vodacom.co.za/docs/
4 https://archibus.vodacom.co.za/examples/
4 https://archibus.vodacom.co.za/Leasure-the-deed-will-the-clipt-Angely-ands-Banq?d=archibus.vodacom.co.za
3 https://archibus.vodacom.co.za/docs/setup.html
3 https://archibus.vodacom.co.za/_Incapsula_Resource?CWUDNSAI=23&xinfo=57-13307322-0%200NNN%20RT%281705258867816%203%29%20q%280%20-1%20-1%20-1%29%20r%280%20-1%29%20B15%284%2c200%2c0%29%20U18&incident_id=168700006022390 1306-81567940232020409&edet=15&cinfo=04000000&rpinfo=0&mth=GET
3 https://archibus.vodacom.co.za/_Incapsula_Resource?CWUDNSAI=23&xinfo=14-34929213-0%200NNN%20RT%281696791682157%204%29%20q%280%20-1%20-1%20-1%29%20r%280%20-1%29%20B15%284%2c200%2c0%29%20U18&incident_id=763001140096022537-173542238158789774&edet=15&cinfo=04000000&rpinfo=0&mth=GET
2 https://archibus.vodacom.co.za/_Incapsula_Resource?CWUDNSAI=23&xinfo=4-71886990-0%200NNN%20RT%281702234922706%202787%29%20q%280%20-1%20-1%201%29%20r%280%20-1%29%20B15%284%2C200%2C0%29%20U18&incident_id=763001220427927261-377042573236838020&edet=15&cinfo=04000000&rpinfo=0&mth=GET
2 https://archibus.vodacom.co.za/_Incapsula_Resource?CWUDNSAI=23&xinfo=12-68759309-0%200NNN%20RT%281686510514654%204%29%20q%280%20-1%20-1%20-1%29%20r%280%20-1%29%20B15%284%2c200%2c0%29%20U18&incident_id=767000350234861307-337740744850606284&edet=15&cinfo=04000000&rpinfo=0&mth=GET
2 https://archibus.vodacom.co.za/host-manager/
2 https://archibus.vodacom.co.za/_Incapsula_Resource?CWUDNSAI=23&xinfo=2-25691562-0%200NNN%20RT%281694372513116%205%29%20q%280%20-1%20-1%20-1%29%20r%280%20-1%29%20B15%284%2c200%2c0%29%20U18&incident_id=451001150135587882-128340275738385602&edet=15&cinfo=04000000&rpinfo=0&mth=GET
2 https://archibus.vodacom.co.za/docs/RELEASE-NOTES.txt
1 https://archibus.vodacom.co.za/docs/service/
1 https://archibus.vodacom.co.za/_Incapsula_Resource?CWUDNSAI=23&xinfo=14-153614192-0%200NNN%20RT%281681066840725%203%29%20q%280%20-1%20-1%20-1%29%20r%280%20-1%29%20B15%284%2c200%2c0%29%20U18&incident_id=768000300342834631-735154962102749070&edet=15&cinfo=04000000&rpinfo=0&mth=GET
1 https://archibus.vodacom.co.za/docs/logs/
1 https://archibus.vodacom.co.za/manager/java/
1 https://archibus.vodacom.co.za/_Incapsula_Resource?CWUDNSAI=23&xinfo=13-243380468-0%200NNN%20RT%281684090859136%203%29%20q%280%20-1%20-1%20-1%29%20r%280%20-1%29%20B15%284%2c200%2c0%29%20U18&incident_id=764000300423775679-1171258712908367757&edet=15&cinfo=04000000&rpinfo=0&mth=GET
1 https://archibus.vodacom.co.za/host-manager/service/
1 https://archibus.vodacom.co.za/_Incapsula_Resource?CWUDNSAI=23%22xinfo=9-63593046-0%200NNN%20RT%2816943725165 02%202831%29%20q%280%20-1%20-1%200%29%20r%280%20-1%29%20B15%284%2c200%2c0%29%20U18%22incident_id=451001150135587882-313333098521763017%22edet=15%22cinfo=04000000%22rpinfo=0%22mth=GET
1 https://archibus.vodacom.co.za/docs/APIs/
1 https://archibus.vodacom.co.za/_Incapsula_Resource?CWUDNSAI=23&xinfo=5-90056699-0%200NNN%20RT%281691953373089%209%29%20q%280%20-1%20-1%20-1%29%20r%280%20-1%29%20B15%284%2C200%2C0%29%20U18&incident_id=451001120180377263-419559953423080453&edet=15&cinfo=04000000&rpinfo=0&mth=GET
1 https://archibus.vodacom.co.za/host-manager/Service/
1 https://archibus.vodacom.co.za/docs/manager-howto.html
1 https://archibus.vodacom.co.za/docs/appdev/APIs/
1 https://archibus.vodacom.co.za/manager/service.asmx?wsdl
1 https://archibus.vodacom.co.za/docs/api/service.asmx?wsdl
1 https://archibus.vodacom.co.za/_Incapsula_Resource?CWUDNSAI=23%22xinfo=11-189604665-0%200NNN%20RT%2816840909218 55%202362%29%20q%280%20-1%20-1%200%29%20r%280%20-1%29%20B15%284%2c200%2c0%29%20U18%22incident_id=764000300423775679-912063067296892811%22edet=15%22cinfo=04000000%22rpinfo=0%22mth=GET
1 https://archibus.vodacom.co.za/docs/service.asmx?wsdl
1 https://archibus.vodacom.co.za/docs/config/ws.asmx?wsdl
1 https://archibus.vodacom.co.za/docs/api/logs/
1 https://archibus.vodacom.co.za/FPRWin/service/
1 https://archibus.vodacom.co.za/_Incapsula_Resource?CWUDNSAI=23&xinfo=11-217099708-0%200NNN%20RT%281688929427421%2010%29%20q%280%20-1%20-1%20-1%29%20r%280%20-1%29%20B15%284%2C200%2C0%29%20U18&incident_id=281000660478098624-104987613815852 6603&edet=15&cinfo=04000000&rpinfo=0&mth=GET
1 https://archibus.vodacom.co.za/manager/service/
1 https://archibus.vodacom.co.za/_Incapsula_Resource?CWUDNSAI=23%22xinfo=13-199918871-0%200NNN%20RT%2816998157311 78%202650%29%20q%280%20-1%20-1%200%29%20r%280%20-1%29%20B15%284%2c200%2c0%29%20U18%22incident_id=128000840526202745-103373459019321 0637%22edet=15%22cinfo=04000000%22rpinfo=0%22mth=GET
1 https://archibus.vodacom.co.za/docs/api/service/
1 https://archibus.vodacom.co.za/docs/ws.asmx?wsdl
1 https://archibus.vodacom.co.za/docs/appdev/service/
1 https://archibus.vodacom.co.za/_Incapsula_Resource?CWUDNSAI=23&xinfo=4-14899366-0%200NNN%20RT%2816967917477 44%202749%29%20q%280%20-1%20-1%200%29%20r%280%20-1%29%20B15%284%2C200%2C0%29%20U18&incident_id=763001140096022537-781033403776441 64&edet=15&cinfo=04000000&rpinfo=0&mth=GET
1 https://archibus.vodacom.co.za/Service/
1 https://archibus.vodacom.co.za/docs/api/
1 https://archibus.vodacom.co.za/_Incapsula_Resource?CWUDNSAI=23&xinfo=9-63593046-0%200NNN%20RT%2816943725165 02%202831%29%20q%280%20-1%20-1%200%29%20r%280%20-1%29%20B15%284%2C200%2C0%29%20U18&incident_id=451001150135587882-313333098521763017&edet=15&cinfo=04000000&rpinfo=0&mth=GET
1 https://archibus.vodacom.co.za/host-manager/APIs/
1 https://archibus.vodacom.co.za/host-manager/ws.asmx?wsdl
1 https://archibus.vodacom.co.za/docs/realm-howto.html
1 https://archibus.vodacom.co.za/examples/api.asmx?wsdl
1 https://archibus.vodacom.co.za/examples/service.asmx?wsdl
1 https://archibus.vodacom.co.za/docs/config/api.asmx?wsdl
1 https://archibus.vodacom.co.za/_Incapsula_Resource?CWUDNSAI=23&xinfo=42-8036113-0%200NNN%20RT%2817052589806 06%202800%29%20q%280%20-1%20-1%202%29%20r%280%20-1%29%20B15%284%2C200%2C0%29%20U18&incident_id=168700006022390 1306-46148676381770154&edet=15&cinfo=04000000&rpinfo=0&mth=GET
1 https://archibus.vodacom.co.za/docs/api/manager/

1 https://archibus.vodacom.co.za/service.asmx?wsdl
1 https://archibus.vodacom.co.za/docs/api/APIs/
1 https://archibus.vodacom.co.za/FPRWin/api.asmx?wsdl
1 https://archibus.vodacom.co.za/docs/api/api.asmx?wsdl
1 https://archibus.vodacom.co.za/manager/html
1 https://archibus.vodacom.co.za/ws.asmx?wsdl
1 https://archibus.vodacom.co.za/_Incapsula_Resource?CWUDNSAI=23&xinfo=11-189604665-0%200NNN%20RT%281684090921855%202362%29%20q%280%20-1%20-1%200%29%20r%280%20-1%29%20B15%284%2C200%2C0%29%20U18&incident_id=764000300423775679-912063067296892811&edet=15&cinfo=04000000&rpinfo=0&mth=GET
1 https://archibus.vodacom.co.za/examples/Service/
1 https://archibus.vodacom.co.za/manager/status
1 https://archibus.vodacom.co.za/docs/config/service/
1 https://archibus.vodacom.co.za/FPRWin/service.asmx?wsdl
1 https://archibus.vodacom.co.za/host-manager/manager/
1 https://archibus.vodacom.co.za/FPRWin/APIs/
1 https://archibus.vodacom.co.za/examples/ws.asmx?wsdl
1 https://archibus.vodacom.co.za/docs/appdev/service.asmx?wsdl
1 https://archibus.vodacom.co.za/_Incapsula_Resource?CWUDNSAI=23&xinfo=9-84466755-0%200NNN%20RT%281691953378741%2023202%29%20q%280%20-1%20-1%200%29%20r%280%20-1%29%20B15%284%2C200%2C0%29%20U18&incident_id=451001120180377263-397119526690561033&edet=15&cinfo=04000000&rpinfo=0&mth=GET
1 https://archibus.vodacom.co.za/docs/Service/
1 https://archibus.vodacom.co.za/host-manager/html
1 https://archibus.vodacom.co.za/docs/appdev/api.asmx?wsdl
1 https://archibus.vodacom.co.za/docs/config/APIs/
1 https://archibus.vodacom.co.za/docs/appdev/ws.asmx?wsdl
1 https://archibus.vodacom.co.za/_Incapsula_Resource?CWUDNSAI=23%22xinfo=9-84466755-0%200NNN%20RT%281691953378741%2023202%29%20q%280%20-1%20-1%200%29%20r%280%20-1%29%20B15%284%2c200%2c0%29%20U18%22incident_id=451001120180377263-397119526690561033%22edet=15%22cinfo=04000000%22rpinfo=0%22mth=GET
1 https://archibus.vodacom.co.za/manager/APIs/
1 https://archibus.vodacom.co.za/examples/APIs/
1 https://archibus.vodacom.co.za/manager/api.asmx?wsdl
1 https://archibus.vodacom.co.za/host-manager/service.asmx?wsdl
1 https://archibus.vodacom.co.za/examples/service/
1 https://archibus.vodacom.co.za/manager/Service/
1 https://archibus.vodacom.co.za/manager/ws.asmx?wsdl
1 https://archibus.vodacom.co.za/docs/config/Service/
1 https://archibus.vodacom.co.za/docs/appdev/java/
1 https://archibus.vodacom.co.za/APIs/
1 https://archibus.vodacom.co.za/docs/config/service.asmx?wsdl
1 https://archibus.vodacom.co.za/docs/api.asmx?wsdl
1 https://archibus.vodacom.co.za/api.asmx?wsdl
1 https://archibus.vodacom.co.za/_Incapsula_Resource?CWUDNSAI=23%22xinfo=9-142984614-0%200NNN%20RT%2816889294274 39%202760%29%20q%280%20-1%20-1%200%29%20r%281%20-1%29%20B15%284%2c200%2c0%29%20U18%22incident_id=28100066047809 8624-688767335294111881%22edet=15%22cinfo=04000000%22rpinfo=0%22mth=GET
1 https://archibus.vodacom.co.za/host-manager/api.asmx?wsdl
1 https://archibus.vodacom.co.za/service/

Total number of unique links that encountered connection errors: 18
Links with highest number of connection errors:
3 https://archibus.vodacom.co.za/examples/
3 https://archibus.vodacom.co.za/docs/changelog.html
3 https://archibus.vodacom.co.za/docs/config/
3 https://archibus.vodacom.co.za/manager/status
2 https://archibus.vodacom.co.za/docs/realm-howto.html
2 https://archibus.vodacom.co.za/host-manager/html
2 https://archibus.vodacom.co.za/FPRWin/index.aspx
2 https://archibus.vodacom.co.za/docs/api/
2 https://archibus.vodacom.co.za/docs/jndi-datasource-examples-howto.html
2 https://archibus.vodacom.co.za/docs/appdev/
1 https://archibus.vodacom.co.za/docs/cluster-howto.html
1 https://archibus.vodacom.co.za/manager/
1 https://archibus.vodacom.co.za/_Incapsula_Resource?CWUDNSAI=23&xinfo=%22'%3E%3Cqss%20a%3DX47672656Y2_1Z%3E&incident_id=764000300423775679-912063067296892811&edet=15&cinfo=04000000&rpinfo=0&mth=GET
1 https://archibus.vodacom.co.za/_Incapsula_Resource?SWKMTFSR=1&e=%22'%3E%3Cqss%20a%3DX140370404099280Y2_1Z%3E
1 https://archibus.vodacom.co.za/_Incapsula_Resource?CWUDNSAI=%22'%3E%3Cqss%20a%3DX47672656Y1_1Z%3E&xinfo=11-189604665-0%200NNN%20RT%2816840909218 55%202362%29%20q%280%20-1%20-1%200%29%20r%280%20-1%29%20B15%284%2C200%2C0%29%20U18&incident_id=764000300423775679-912063067296892811&edet=15&cinfo=04000000&rpinfo=0&mth=GET
1 https://archibus.vodacom.co.za/docs/setup.html
1 https://archibus.vodacom.co.za/docs/manager-howto.html
1 https://archibus.vodacom.co.za/_Incapsula_Resource?SWKMTFSR=%22'%3E%3Cqss%20a%3DX140370404099280Y1_1Z%3E&e=0.5329770916436014

Phase wise summary of timeout and connection errors encountered:
ePhaseWSDirectoryPathTests : 24 0
ePhaseWSEnumeration : 25 0
ePhaseParameterTests : 0 4
ePhaseWebCgiOob : 28 0
ePhaseCookieTests : 21 10
ePhaseHeaderTests : 21 18
ePhasePathTests : 6 0

150009 Links Crawled (1)

150009 Links Crawled

archibus.vodacom.co.za

Finding #	10510093	**Severity**	Information Gathered - Level 1
Unique #			

WAS Web Application Report

10422296-2d4e-40fa-a8d8-27ad9700956b

Group	Scan Diagnostics		
CWE	-	**Detection Date**	11 Feb 2024 21:02 GMT+0200
OWASP	-		
WASC	-		

Details

Threat

The list of unique links crawled and HTML forms submitted by the scanner appear in the Results section. This list may contain fewer links than the maximum threshold defined.

NOTE: This list also includes:
- All the unique links that are reported in QID 150140 (Redundant links/URL paths crawled and not crawled)
- All the forms reported in QID 150152 (Forms Crawled)
- All the forms in QID 150115 (Authentication Form Found)
- Certain requests from QID 150172 (Requests Crawled)

Impact

N/A

Solution

N/A

Results

Duration of crawl phase (seconds): 1681.00
Number of links: 80
(This number excludes form requests, ajax links (included in QID 150148) and links re-requested during authentication.)

https://archibus.vodacom.co.za/
https://archibus.vodacom.co.za/FPRWin/
https://archibus.vodacom.co.za/FPRWin/index.aspx
https://archibus.vodacom.co.za/_Incapsula_Resource?CWUDNSAI=23%22xinfo=10-42257572-0%200NNN%20RT%281686510627231%202271%29%20q%280%20-1%20-1%200%29%20r%280%20-1%29%20B15%284%2c200%2c0%29%20U18%22incident_id=767000350234861307-207301230861420746%22edet=15%22cinfo=04000000%22rpinfo=0%22mth=GET
https://archibus.vodacom.co.za/_Incapsula_Resource?CWUDNSAI=23%22xinfo=11-189604665-0%200NNN%20RT%281684090921855%202362%29%20q%280%20-1%20-1%200%29%20r%280%20-1%29%20B15%284%2c200%2c0%29%20U18%22incident_id=764000300423775679-912063067296892811%22edet=15%22cinfo=04000000%22rpinfo=0%22mth=GET
https://archibus.vodacom.co.za/_Incapsula_Resource?CWUDNSAI=23%22xinfo=13-199918871-0%200NNN%20RT%281699815731178%202650%29%20q%280%20-1%20-1%200%29%20r%280%20-1%29%20B15%284%2C200%2C0%29%20U18%22incident_id=128000840526202745-103373459019321063 7%22edet=15%22cinfo=04000000%22rpinfo=0%22mth=GET
https://archibus.vodacom.co.za/_Incapsula_Resource?CWUDNSAI=23%22xinfo=13-199918871-0%200NNN%20RT%281699815731178%202650%29%20q%280%20-1%20-1%200%29%20r%280%20-1%29%20B15%284%2c200%2c0%29%20U18%22incident_id=128000840526202745-103373459019321063 7%22edet=15%22cinfo=04000000%22rpinfo=0%22mth=GET
https://archibus.vodacom.co.za/_Incapsula_Resource?CWUDNSAI=23%22xinfo=3-56251934-0%200NNN%20RT%281691953375915%209%29%20q%280%20-1%20-1%200%29%20r%280%20-1%29%20B15%284%2C200%2C0%29%20U18%22incident_id=45100112018037726 3-267491121570192387%22edet=15%22cinfo=04000000%22rpinfo=0%22mth=GET
https://archibus.vodacom.co.za/_Incapsula_Resource?CWUDNSAI=23%22xinfo=3-56251934-0%200NNN%20RT%281691953375915%209%29%20q%280%20-1%20-1%200%29%20r%280%20-1%29%20B15%284%2c200%2c0%29%20U18%22incident_id=45100112018037726 3-267491121570192387%22edet=15%22cinfo=04000000%22rpinfo=0%22mth=GET
https://archibus.vodacom.co.za/_Incapsula_Resource?CWUDNSAI=23%22xinfo=4-14899366-0%200NNN%20RT%281696791747744%202749%29%20q%280%20-1%20-1%200%29%20r%280%20-1%29%20B15%284%2C200%2C0%29%20U18%22incident_id=763001140096022537-78103340377644164%22edet=15%22cinfo=04000000%22rpinfo=0%22mth=GET
https://archibus.vodacom.co.za/_Incapsula_Resource?CWUDNSAI=23%22xinfo=4-14899366-0%200NNN%20RT%281696791747744%202749%29%20q%280%20-1%20-1%200%29%20r%280%20-1%29%20B15%284%2c200%2c0%29%20U18%22incident_id=763001140096022537-78103340377644164%22edet=15%22cinfo=04000000%22rpinfo=0%22mth=GET
https://archibus.vodacom.co.za/_Incapsula_Resource?CWUDNSAI=23%22xinfo=4-71886990-0%200NNN%20RT%281702234922706%202787%29%20q%280%20-1%20-1%201%29%20r%280%20-1%29%20B15%284%2c200%2c0%29%20U18%22incident_id=763001220427927261-377042573236838020%22edet=15%22cinfo=04000000%22rpinfo=0%22mth=GET
https://archibus.vodacom.co.za/_Incapsula_Resource?CWUDNSAI=23%22xinfo=42-8036113-0%200NNN%20RT%281705258980606%202800%29%20q%280%20-1%20-1%202%29%20r%280%20-1%29%20B15%284%2c200%2c0%29%20U18%22incident_id=168700006022390 1306-46148676381770154%22edet=15%22cinfo=04000000%22rpinfo=0%22mth=GET
https://archibus.vodacom.co.za/_Incapsula_Resource?CWUDNSAI=23%22xinfo=9-142984614-0%200NNN%20RT%281688929427439%202760%29%20q%280%20-1%20-1%200%29%20r%281%20-1%29%20B15%284%2c200%2c0%29%20U18%22incident_id=281000660478098624-688767335294111881%22edet=15%22cinfo=04000000%22rpinfo=0%22mth=GET
https://archibus.vodacom.co.za/_Incapsula_Resource?CWUDNSAI=23%22xinfo=9-63593046-0%200NNN%20RT%281694372516502%202831%29%20q%280%20-1%20-1%200%29%20r%280%20-1%29%20B15%284%2c200%2c0%29%20U18%22incident_id=451001150135587882-313333098521763017%22edet=15%22cinfo=04000000%22rpinfo=0%22mth=GET
https://archibus.vodacom.co.za/_Incapsula_Resource?CWUDNSAI=23%22xinfo=9-84466755-0%200NNN%20RT%281691953378741%2023202%29%20q%280%20-1%20-1%200%29%20r%280%20-1%29%20B15%284%2c200%2c0%29%20U18%22incident_id=451001120180377263-397119526690561033%22edet=15%22cinfo=04000000%22rpinfo=0%22mth=GET
https://archibus.vodacom.co.za/_Incapsula_Resource?CWUDNSAI=23&xinfo=10-42257572-0%200NNN%20RT%281686510627231%202271%29%20q%280%20-1%20-1%200%29%20r%280%20-1%29%20B15%284%2C200%2C0%29%20U18&incident_id=767000350234861307-207301230861420746&edet=15&cinfo=04000000&rpinfo=0&mth=GET
https://archibus.vodacom.co.za/_Incapsula_Resource?CWUDNSAI=23&xinfo=10-97597847-0%200NNN%20RT%281691953271388%207%29%20q%280%20-1%20-1%20-1%29%20r%280%20-1%29%20B15%284%2C200%2C0%29%20U18&incident_id=451001120180377263-459868152776563722&edet=15&cinfo=04000000&rpinfo=0&mth=GET
https://archibus.vodacom.co.za/_Incapsula_Resource?CWUDNSAI=23&xinfo=10-97597847-0%200NNN%20RT%281691953271388%207%29%20q%280%20-1%20-1%20-1%29%20r%280%20-1%29%20B15%284%2c200%2c0%29%20U18&incident_id=451001120180377263-459868152776563722&edet=15&cinfo=04000000&rpinfo=0&mth=GET
https://archibus.vodacom.co.za/_Incapsula_Resource?CWUDNSAI=23&xinfo=11-189604665-0%200NNN%20RT%281684090921855%202362%29%20q%280%20-1%20-1%200%29%20r%280%20-1%29%20B15%284%2C200%2C0%29%20U18&incident_id=764000300423775679-912063067296892811&edet=15&cinfo=04000000&rpinfo=0&mth=GET
https://archibus.vodacom.co.za/_Incapsula_Resource?CWUDNSAI=23&xinfo=11-217099708-0%200NNN%20RT%281688929427421%2010%29%20q%280%20-1%20-1%20-1%29%20r%280%20-1%29%20B15%284%2C200%2C0%29%20U18&incident_id=281000660478098624-104987613815852660 3&edet=15&cinfo=04000000&rpinfo=0&mth=GET
https://archibus.vodacom.co.za/_Incapsula_Resource?CWUDNSAI=23&xinfo=11-61474434-0%200NNN%20RT%281686510627214%209%29%20q%280%20-1%20-1%20-1%29%20r

WAS Web Application Report

%280%20-1%29%20B15%284%2C200%2C0%29%20U18&incident_id=767000350234861307-302640446746593483&edet=15&cinfo=04000000&rpinfo=0&mth=GET
https://archibus.vodacom.co.za/_Incapsula_Resource?CWUDNSAI=23&xinfo=11-93784308-0%200NNN%20RT%281702234859957%2012%29%20q%280%20-1%20-1%20-1%29%20r
%280%20-1%29%20B15%284%2c200%2c0%29%20U18&incident_id=763001220427927261-4900731975008989555&edet=15&cinfo=04000000&rpinfo=0&mth=GET
https://archibus.vodacom.co.za/_Incapsula_Resource?CWUDNSAI=23&xinfo=12-217098056-0%200NNN%20RT%281684090921837%2011%29%20q%280%20-1%20-1%20-1%29%20r
%280%20-1%29%20B15%284%2C200%2C0%29%20U18&incident_id=764000300423775679-103281847800561857 2&edet=15&cinfo=04000000&rpinfo=0&mth=GET
https://archibus.vodacom.co.za/_Incapsula_Resource?CWUDNSAI=23&xinfo=12-32525279-0%200NNN%20RT%281696791747727%209%29%20q%280%20-1%20-1%20-1%29%20r
%280%20-1%29%20B15%284%2C200%2C0%29%20U18&incident_id=763001140096022537-164225543560699020&edet=15&cinfo=04000000&rpinfo=0&mth=GET
https://archibus.vodacom.co.za/_Incapsula_Resource?CWUDNSAI=23&xinfo=12-68759309-0%200NNN%20RT%281686510514654%204%29%20q%280%20-1%20-1%20-1%29%20r
%280%20-1%29%20B15%284%2c200%2c0%29%20U18&incident_id=767000350234861307-337740744850606284&edet=15&cinfo=04000000&rpinfo=0&mth=GET
https://archibus.vodacom.co.za/_Incapsula_Resource?CWUDNSAI=23&xinfo=13-199918871-0%200NNN%20RT%281699815731178%202650%29%20q%280%20-1%20-1%200%29%20r
%280%20-1%29%20B15%284%2C200%2C0%29%20U18&incident_id=128000840526202745-1033734590193210637&edet=15&cinfo=04000000&rpinfo=0&mth=GET
https://archibus.vodacom.co.za/_Incapsula_Resource?CWUDNSAI=23&xinfo=13-243380468-0%200NNN%20RT%281684090859136%203%29%20q%280%20-1%20-1%20-1%29%20r
%280%20-1%29%20B15%284%2c200%2c0%29%20U18&incident_id=764000300423775679-117125871290836775 7&edet=15&cinfo=04000000&rpinfo=0&mth=GET
https://archibus.vodacom.co.za/_Incapsula_Resource?CWUDNSAI=23&xinfo=14-153614192-0%200NNN%20RT%281681066840725%203%29%20q%280%20-1%20-1%20-1%29%20r
%280%20-1%29%20B15%284%2c200%2c0%29%20U18&incident_id=768000300342834631-7351549621027490 70&edet=15&cinfo=04000000&rpinfo=0&mth=GET
https://archibus.vodacom.co.za/_Incapsula_Resource?CWUDNSAI=23&xinfo=14-34929213-0%200NNN%20RT%281696791682157%204%29%20q%280%20-1%20-1%20-1%29%20r
%280%20-1%29%20B15%284%2c200%2c0%29%20U18&incident_id=763001140096022537-173542238158789774&edet=15&cinfo=04000000&rpinfo=0&mth=GET
https://archibus.vodacom.co.za/_Incapsula_Resource?CWUDNSAI=23&xinfo=2-25691562-0%200NNN%20RT%281694372513116%205%29%20q%280%20-1%20-1%20-1%29%20r
%280%20-1%29%20B15%284%2c200%2c0%29%20U18&incident_id=451001150135587882-128340275738385602&edet=15&cinfo=04000000&rpinfo=0&mth=GET
https://archibus.vodacom.co.za/_Incapsula_Resource?CWUDNSAI=23&xinfo=3-56251934-0%200NNN%20RT%281691953375915%209%29%20q%280%20-1%20-1%200%29%20r
%280%20-1%29%20B15%284%2C200%2C0%29%20U18&incident_id=451001120180377263-267491121570192387&edet=15&cinfo=04000000&rpinfo=0&mth=GET
https://archibus.vodacom.co.za/_Incapsula_Resource?CWUDNSAI=23&xinfo=4-14899366-0%200NNN%20RT%281696791747744%202749%29%20q%280%20-1%20-1%200%29%20r
%280%20-1%29%20B15%284%2C200%2C0%29%20U18&incident_id=763001140096022537-781033403776441 64&edet=15&cinfo=04000000&rpinfo=0&mth=GET
https://archibus.vodacom.co.za/_Incapsula_Resource?CWUDNSAI=23&xinfo=4-71886990-0%200NNN%20RT%281702234922706%202787%29%20q%280%20-1%20-1%201%29%20r
%280%20-1%29%20B15%284%2C200%2C0%29%20U18&incident_id=763001220427927261-377042573236838020&edet=15&cinfo=04000000&rpinfo=0&mth=GET
https://archibus.vodacom.co.za/_Incapsula_Resource?CWUDNSAI=23&xinfo=42-8036113-0%200NNN%20RT%281705258980606%202800%29%20q%280%20-1%20-1%202%29%20r
%280%20-1%29%20B15%284%2C200%2C0%29%20U18&incident_id=168700006022390 1306-461486763817701 54&edet=15&cinfo=04000000&rpinfo=0&mth=GET
https://archibus.vodacom.co.za/_Incapsula_Resource?CWUDNSAI=23&xinfo=5-13169156-0%200NNN%20RT%281705258980589%2010%29%20q%280%20-1%20-1%20-1%29%20r
%280%20-1%29%20B15%284%2C200%2C0%29%20U18&incident_id=168700006022390 1306-796864052539559 73&edet=15&cinfo=04000000&rpinfo=0&mth=GET
https://archibus.vodacom.co.za/_Incapsula_Resource?CWUDNSAI=23&xinfo=5-88290743-0%200NNN%20RT%281702234922688%2010%29%20q%280%20-1%20-1%20-1%29%20r
%280%20-1%29%20B15%284%2C200%2C0%29%20U18&incident_id=763001220427927261-459666233499524741&edet=15&cinfo=04000000&rpinfo=0&mth=GET
https://archibus.vodacom.co.za/_Incapsula_Resource?CWUDNSAI=23&xinfo=5-90056699-0%200NNN%20RT%281691953373089%209%29%20q%280%20-1%20-1%20-1%29%20r
%280%20-1%29%20B15%284%2C200%2C0%29%20U18&incident_id=451001120180377263-419559953423080453&edet=15&cinfo=04000000&rpinfo=0&mth=GET
https://archibus.vodacom.co.za/_Incapsula_Resource?CWUDNSAI=23&xinfo=5-94420317-0%200NNN%20RT%281681066890090%2010%29%20q%280%20-1%20-1%20-1%29%20r
%281%20-1%29%20B15%284%2C200%2C0%29%20U18&incident_id=768000300342834631-449961922398259077&edet=15&cinfo=04000000&rpinfo=0&mth=GET
https://archibus.vodacom.co.za/_Incapsula_Resource?CWUDNSAI=23&xinfo=5-94420320-0%200NNN%20RT%281681066890106%202879%29%20q%280%20-1%20-1%200%29%20r
%280%20-1%29%20B15%284%2C200%2C0%29%20U18&incident_id=768000300342834631-449963447111649157&edet=15&cinfo=04000000&rpinfo=0&mth=GET
https://archibus.vodacom.co.za/_Incapsula_Resource?CWUDNSAI=23&xinfo=5-94420320-0%200NNN%20RT%281681066890106%202879%29%20q%280%20-1%20-1%200%29%20r
%280%20-1%29%20B15%284%2c200%2c0%29%20U18&incident_id=768000300342834631-449963447111649157&edet=15&cinfo=04000000&rpinfo=0&mth=GET
https://archibus.vodacom.co.za/_Incapsula_Resource?CWUDNSAI=23&xinfo=57-13307322-0%200NNN%20RT%281705258867816%203%29%20q%280%20-1%20-1%20-1%29%20r
%280%20-1%29%20B15%284%2c200%2c0%29%20U18&incident_id=168700006022390 1306-815679402320 2409&edet=15&cinfo=04000000&rpinfo=0&mth=GET
https://archibus.vodacom.co.za/_Incapsula_Resource?CWUDNSAI=23&xinfo=6-56552911-0%200NNN%20RT%281699815672206%205%29%20q%280%20-1%20-1%20-1%29%20r
%280%20-1%29%20B15%284%2c200%2c0%29%20U18&incident_id=128000840526202745-294015529604093190&edet=15&cinfo=04000000&rpinfo=0&mth=GET
https://archibus.vodacom.co.za/_Incapsula_Resource?CWUDNSAI=23&xinfo=8-36670336-0%200NNN%20RT%281694372516485%209%29%20q%280%20-1%20-1%20-1%29%20r
%280%20-1%29%20B15%284%2C200%2C0%29%20U18&incident_id=451001150135587882-181277968159677640&edet=15&cinfo=04000000&rpinfo=0&mth=GET
https://archibus.vodacom.co.za/_Incapsula_Resource?CWUDNSAI=23&xinfo=8-86225779-0%200NNN%20RT%281699815731158%2013%29%20q%280%20-1%20-1%20-1%29%20r
%280%20-1%29%20B15%284%2C200%2C0%29%20U18&incident_id=128000840526202745-446159613578974472&edet=15&cinfo=04000000&rpinfo=0&mth=GET
https://archibus.vodacom.co.za/_Incapsula_Resource?CWUDNSAI=23&xinfo=9-142966740-0%200NNN%20RT%281688929314974%202%29%20q%280%20-1%20-1%20-1%29%20r
%280%20-1%29%20B15%284%2c200%2c0%29%20U18&incident_id=281000660478098624-688680993566560393&edet=15&cinfo=04000000&rpinfo=0&mth=GET
https://archibus.vodacom.co.za/_Incapsula_Resource?CWUDNSAI=23&xinfo=9-142984614-0%200NNN%20RT%281688929427439%202760%29%20q%280%20-1%20-1%200%29%20r
%281%20-1%29%20B15%284%2C200%2C0%29%20U18&incident_id=281000660478098624-688767335294111881&edet=15&cinfo=04000000&rpinfo=0&mth=GET
https://archibus.vodacom.co.za/_Incapsula_Resource?CWUDNSAI=23&xinfo=9-63593046-0%200NNN%20RT%281694372516502%202831%29%20q%280%20-1%20-1%200%29%20r
%280%20-1%29%20B15%284%2C200%2C0%29%20U18&incident_id=451001150135587882-313333098521763017&edet=15&cinfo=04000000&rpinfo=0&mth=GET
https://archibus.vodacom.co.za/_Incapsula_Resource?CWUDNSAI=23&xinfo=9-84466755-0%200NNN%20RT%281691953378741%2023202%29%20q%280%20-1%20-1%200%29%20r
%280%20-1%29%20B15%284%2C200%2C0%29%20U18&incident_id=451001120180377263-397119526690561033&edet=15&cinfo=04000000&rpinfo=0&mth=GET
https://archibus.vodacom.co.za/_Incapsula_Resource?SWKMTFSR=1&e=0.4472103130471645
https://archibus.vodacom.co.za/_Incapsula_Resource?SWKMTFSR=1&e=0.4981508946970825
https://archibus.vodacom.co.za/_Incapsula_Resource?SWKMTFSR=1&e=0.5329770916436014
https://archibus.vodacom.co.za/_Incapsula_Resource?SWKMTFSR=1&e=0.6767940789579447
https://archibus.vodacom.co.za/_Incapsula_Resource?SWKMTFSR=1&e=0.7227896506086273
https://archibus.vodacom.co.za/_Incapsula_Resource?SWKMTFSR=1&e=0.7902679497011122
https://archibus.vodacom.co.za/_Incapsula_Resource?SWKMTFSR=1&e=0.8560383602618578
https://archibus.vodacom.co.za/_Incapsula_Resource?SWKMTFSR=1&e=0.913395824408842
https://archibus.vodacom.co.za/csp_report
https://archibus.vodacom.co.za/docs/
https://archibus.vodacom.co.za/docs/RELEASE-NOTES.txt
https://archibus.vodacom.co.za/docs/api/
https://archibus.vodacom.co.za/docs/api/index.html
https://archibus.vodacom.co.za/docs/appdev/
https://archibus.vodacom.co.za/docs/changelog.html
https://archibus.vodacom.co.za/docs/cluster-howto.html
https://archibus.vodacom.co.za/docs/config/
https://archibus.vodacom.co.za/docs/deployer-howto.html
https://archibus.vodacom.co.za/docs/jndi-datasource-examples-howto.html
https://archibus.vodacom.co.za/docs/manager-howto.html
https://archibus.vodacom.co.za/docs/realm-howto.html
https://archibus.vodacom.co.za/docs/security-howto.html
https://archibus.vodacom.co.za/docs/setup.html
https://archibus.vodacom.co.za/examples/
https://archibus.vodacom.co.za/favicon.ico
https://archibus.vodacom.co.za/host-manager/
https://archibus.vodacom.co.za/host-manager/html
https://archibus.vodacom.co.za/manager/
https://archibus.vodacom.co.za/manager/html
https://archibus.vodacom.co.za/manager/status

https://archibus.vodacom.co.za/null

150010 External Links Discovered (1)

150010 External Links Discovered

archibus.vodacom.co.za

Finding #	10510090	**Severity**	Information Gathered - Level 1
Unique #	9215f953-4cb6-47a0-b4db-76b0b01aa471		
Group	Scan Diagnostics		
CWE	-	**Detection Date**	11 Feb 2024 21:02 GMT+0200
OWASP	-		
WASC	-		

Details

Threat

External links discovered during the scan are listed in the Results section. These links were out of scope for the scan and were not crawled.

Impact

N/A

Solution

N/A

Results

Number of links: 32
https://www.imperva.com/why-am-i-seeing-this-page/?src=23%22utm_source=blockingpages
https://www.imperva.com/why-am-i-seeing-this-page/?src=23&utm_source=blockingpages
https://github.com/apache/tomcat/tree/9.0.x
https://fonts.gstatic.com/s/inter/v13/UcC73FwrK3iLTeHuS_fvQtMwCp50KnMa1ZL7.woff2
https://fonts.googleapis.com/css2?family=Inter:wght@300;400;500;700%22display=swap
https://fonts.googleapis.com/css2?family=Inter:wght@300;400;500;700&display=swap
https://wiki.apache.org/tomcat/FrontPage
https://wiki.apache.org/tomcat/Specifications
https://wiki.apache.org/tomcat/TomcatVersions
https://tomcat.apache.org/
https://tomcat.apache.org/bugreport.html
https://tomcat.apache.org/connectors-doc/
https://tomcat.apache.org/contact.html
https://tomcat.apache.org/download-connectors.cgi
https://tomcat.apache.org/download-native.cgi
https://tomcat.apache.org/faq/
https://tomcat.apache.org/findhelp.html
https://tomcat.apache.org/getinvolved.html
https://tomcat.apache.org/heritage.html
https://tomcat.apache.org/legal.html
https://tomcat.apache.org/lists.html
https://tomcat.apache.org/migration.html
https://tomcat.apache.org/native-doc/
https://tomcat.apache.org/resources.html
https://tomcat.apache.org/security.html
https://tomcat.apache.org/source.html
https://tomcat.apache.org/taglibs/
https://tomcat.apache.org/whoweare.html
https://www.apache.org/
https://www.apache.org/foundation/sponsorship.html
https://www.apache.org/foundation/thanks.html
http://go.microsoft.com/fwlink/?linkid=66138%22clcid%3D0x409

150020 Links Rejected By Crawl Scope or Exclusion List (1)

150020 Links Rejected By Crawl Scope or Exclusion List

archibus.vodacom.co.za

Finding #	10510077	**Severity**	Information Gathered - Level 1

Unique #	9dfa9df4-ca0d-42c1-8c58-06e3d0d2d54a		
Group	Scan Diagnostics		
CWE	-	**Detection Date**	11 Feb 2024 21:02 GMT+0200
OWASP	-		
WASC	-		

Details

Threat

One or more links were not crawled because of an explicit rule to exclude them. This also occurs if a link is malformed.

Exclude list and Include list entries can cause links to be rejected. If a scan is limited to a specific starting directory, then links outside that directory will neither be crawled or tested.

Links that contain a host name or IP address different from the target application are considered external links and not crawled by default; those types of links are not listed here. This often happens when the scope of a scan is limited to the directory of the starting URL. The scope can be changed in the Web Application Record.

During the test phase, some path-based tests may be rejected if the scan is limited to the directory of the starting URL and the test would fall outside that directory. In these cases, the number of rejected links may be too high to list in the Results section.

Impact

Links listed here were neither crawled or tested by the Web application scanning engine.

Solution

A link might have been intentionally matched by a exclude or include list entry. Verify that no links in this list were unintentionally rejected.

Results

Links not permitted:
(This list includes links from QIDs: 150010,150041,150143,150170)

External links discovered:
https://www.imperva.com/why-am-i-seeing-this-page/?src=23%22utm_source=blockingpages
https://www.imperva.com/why-am-i-seeing-this-page/?src=23&utm_source=blockingpages
https://github.com/apache/tomcat/tree/9.0.x
https://fonts.gstatic.com/s/inter/v13/UcC73FwrK3iLTeHuS_fvQtMwCp50KnMa1ZL7.woff2
https://fonts.googleapis.com/css2?family=Inter:wght@300;400;500;700%22display=swap
https://fonts.googleapis.com/css2?family=Inter:wght@300;400;500;700&display=swap
https://wiki.apache.org/tomcat/FrontPage
https://wiki.apache.org/tomcat/Specifications
https://wiki.apache.org/tomcat/TomcatVersions
https://tomcat.apache.org/

IP based excluded links:
Links rejected during the test phase not reported due to volume of links.

150021 Scan Diagnostics (1)

150021 Scan Diagnostics *archibus.vodacom.co.za*

Finding #	10510078	**Severity**	Information Gathered - Level 1
Unique #	734cea3e-ae1c-41dd-9d27-a12d8bdad1e5		
Group	Scan Diagnostics		
CWE	-	**Detection Date**	11 Feb 2024 21:02 GMT+0200
OWASP	-		
WASC	-		

WAS Web Application Report

Details

Threat

This check provides various details of the scan's performance and behavior. In some cases, this check can be used to identify problems that the scanner encountered when crawling the target Web application.

Impact

The scan diagnostics data provides technical details about the crawler's performance and behavior. This information does not necessarily imply problems with the Web application.

Solution

No action is required.

Results

Loaded 4 exclude list entries.
Loaded 0 allow list entries.
HTML form authentication unavailable, no WEBAPP entry found
Target web application page https://archibus.vodacom.co.za/ fetched. Status code:302, Content-Type:text/html, load time:1 milliseconds.
Batch #0 VirtualHostDiscovery: estimated time < 10 minutes (70 tests, 0 inputs)
VirtualHostDiscovery: 70 vulnsigs tests, completed 70 requests, 1013 seconds. Completed 70 requests of 70 estimated requests (100%). All tests completed.
Batch #0 SameSiteScripting: estimated time < 1 minute (2 tests, 0 inputs)
SameSiteScripting: 2 vulnsigs tests, completed 2 requests, 0 seconds. Completed 2 requests of 2 estimated requests (100%). All tests completed.
Batch #0 CMSDetection: estimated time < 10 minutes (1 tests, 1 inputs)
[CMSDetection phase] : No potential CMS found using Blind Elephant algorithm. Aborting the CMS Detection phase
CMSDetection: 1 vulnsigs tests, completed 56 requests, 86 seconds. Completed 56 requests of 56 estimated requests (100%). All tests completed.
No more requeues, redundant link threshold has been surpassed.
Collected 114 links overall in 0 hours 28 minutes duration.
Batch #0 BannersVersionReporting: estimated time < 1 minute (1 tests, 1 inputs)
BannersVersionReporting: 1 vulnsigs tests, completed 0 requests, 0 seconds. Completed 0 requests of 1 estimated requests (0%). All tests completed.
Path manipulation: Estimated requests (payloads x links): files with extension:(0 x 12) + files:(0 x 71) + directories:(9 x 9) + paths:(0 x 80) = total (81)
Batch #0 WS Directory Path manipulation: estimated time < 1 minute (9 tests, 80 inputs)
WS Directory Path manipulation: 9 vulnsigs tests, completed 24 requests, 240 seconds. Completed 24 requests of 81 estimated requests (29.6296%). Some tests were skipped due to errors.
Batch #0 WS enumeration: estimated time < 10 minutes (11 tests, 80 inputs)
WS enumeration: 11 vulnsigs tests, completed 25 requests, 300 seconds. Completed 25 requests of 880 estimated requests (2.84091%). Some tests were skipped due to errors.
Batch #1 URI parameter manipulation (no auth): estimated time < 10 minutes (125 tests, 9 inputs)
Batch #1 URI parameter manipulation (no auth): 125 vulnsigs tests, completed 1107 requests, 27 seconds. Completed 1107 requests of 1125 estimated requests (98.4%). All tests completed.
Batch #1 URI parameter name manipulation (no auth): estimated time < 10 minutes (125 tests, 9 inputs)
Batch #1 URI parameter name manipulation (no auth): 125 vulnsigs tests, completed 246 requests, 1 seconds. Completed 246 requests of 1125 estimated requests (21.8667%). All tests completed.
Batch #1 URI blind SQL manipulation (no auth): estimated time < 1 minute (13 tests, 9 inputs)
Batch #1 URI blind SQL manipulation (no auth): 13 vulnsigs tests, completed 288 requests, 0 seconds. Completed 288 requests of 351 estimated requests (82.0513%). All tests completed.
Batch #1 URI parameter time-based tests (no auth): estimated time < 1 minute (19 tests, 9 inputs)
Batch #1 URI parameter time-based tests (no auth): 19 vulnsigs tests, completed 171 requests, 1 seconds. Completed 171 requests of 171 estimated requests (100%). All tests completed.
Batch #1 URI parameter time-based tests for Apache Struts Vulnerabilities (no auth): estimated time < 1 minute (1 tests, 9 inputs)
Batch #1 URI parameter time-based tests for Apache Struts Vulnerabilities (no auth): 1 vulnsigs tests, completed 9 requests, 0 seconds. Completed 9 requests of 9 estimated requests (100%). All tests completed.
Batch #4 WebCgiOob: estimated time < 30 minutes (133 tests, 1 inputs)
Batch #4 WebCgiOob: 133 vulnsigs tests, completed 155 requests, 397 seconds. Completed 155 requests of 12400 estimated requests (1.25%). All tests completed.
No XML requests found. Skipping XXE tests.
Batch #4 DOM XSS exploitation: estimated time < 1 minute (4 tests, 0 inputs)
Batch #4 DOM XSS exploitation: 4 vulnsigs tests, completed 0 requests, 1 seconds. No tests to execute.
Batch #4 HTTP call manipulation: estimated time < 1 minute (59 tests, 0 inputs)
Batch #4 HTTP call manipulation: 59 vulnsigs tests, completed 0 requests, 0 seconds. No tests to execute.
Batch #4 Open Redirect analysis: estimated time < 1 minute (2 tests, 2 inputs)
Batch #4 Open Redirect analysis: 2 vulnsigs tests, completed 4 requests, 23 seconds. Completed 4 requests of 4 estimated requests (100%). All tests completed.
CSRF tests will not be launched because the scan is not successfully authenticated.
Batch #4 File Inclusion analysis: estimated time < 1 minute (1 tests, 81 inputs)
Batch #4 File Inclusion analysis: 1 vulnsigs tests, completed 0 requests, 0 seconds. Completed 0 requests of 81 estimated requests (0%). All tests completed.
Batch #4 Cookie manipulation: estimated time < 10 minutes (76 tests, 4 inputs)
Batch #4 Cookie manipulation: 76 vulnsigs tests, completed 4884 requests, 687 seconds. Completed 4884 requests of 6968 estimated requests (70.0918%). Some tests were skipped due to errors.
Batch #4 Header manipulation: estimated time < 1 hour (76 tests, 67 inputs)
Batch #4 Header manipulation: 76 vulnsigs tests, completed 11548 requests, 806 seconds. Completed 11548 requests of 27336 estimated requests (42.2447%). Some tests were skipped due to errors.
Batch #4 shell shock detector: estimated time < 1 minute (1 tests, 67 inputs)
Batch #4 shell shock detector: 1 vulnsigs tests, completed 91 requests, 34 seconds. Completed 91 requests of 67 estimated requests (135.821%). All tests completed.
Batch #4 shell shock detector(form): estimated time < 1 minute (1 tests, 0 inputs)
Batch #4 shell shock detector(form): 1 vulnsigs tests, completed 0 requests, 0 seconds. No tests to execute.
Login Brute Force manipulation estimated time: no tests enabled
Login Brute Force manipulation estimated time: no tests enabled
Batch #5 HTTP Time Bandit: estimated time < 1 minute (1 tests, 10 inputs)
Batch #5 HTTP Time Bandit: 1 vulnsigs tests, completed 200 requests, 35 seconds. No tests to execute.
Path manipulation: Estimated requests (payloads x links): files with extension:(1 x 12) + files:(0 x 71) + directories:(4 x 9) + paths:(14 x 80) = total (1168)
Batch #5 Path XSS manipulation: estimated time < 1 minute (19 tests, 80 inputs)
Batch #5 Path XSS manipulation: 19 vulnsigs tests, completed 440 requests, 16 seconds. Completed 440 requests of 1168 estimated requests (37.6712%). All tests completed.
Path manipulation: Estimated requests (payloads x links): files with extension:(0 x 12) + files:(0 x 71) + directories:(1 x 9) + paths:(0 x 80) = total (9)
Batch #5 Tomcat Vuln manipulation: estimated time < 1 minute (1 tests, 80 inputs)

Batch #5 Tomcat Vuln manipulation: 1 vulnsigs tests, completed 8 requests, 0 seconds. Completed 8 requests of 9 estimated requests (88.8889%). All tests completed.
Path manipulation: Estimated requests (payloads x links): files with extension:(0 x 12) + files:(0 x 71) + directories:(16 x 9) + paths:(0 x 80) = total (144)
Batch #5 Time based path manipulation: estimated time < 1 minute (16 tests, 81 inputs)
Batch #5 Time based path manipulation: 16 vulnsigs tests, completed 64 requests, 0 seconds. Completed 64 requests of 144 estimated requests (44.4444%). All tests completed.
Path manipulation: Estimated requests (payloads x links): files with extension:(4 x 12) + files:(18 x 71) + directories:(152 x 9) + paths:(19 x 80) = total (4214)
Batch #5 Path manipulation: estimated time < 10 minutes (193 tests, 80 inputs)
Batch #5 Path manipulation: 193 vulnsigs tests, completed 1835 requests, 160 seconds. Completed 1835 requests of 4214 estimated requests (43.5453%). All tests completed.
Batch #5 WebCgiHrs: estimated time < 1 minute (1 tests, 1 inputs)
Batch #5 WebCgiHrs: 1 vulnsigs tests, completed 3 requests, 0 seconds. Completed 3 requests of 160 estimated requests (1.875%). All tests completed.
Batch #5 WebCgiGeneric: estimated time < 1 hour (451 tests, 1 inputs)
Batch #5 WebCgiGeneric: 451 vulnsigs tests, completed 6075 requests, 537 seconds. Completed 6075 requests of 48400 estimated requests (12.5517%). All tests completed.
Batch #5 Open Redirect analysis: estimated time < 1 minute (2 tests, 2 inputs)
Batch #5 Open Redirect analysis: 2 vulnsigs tests, completed 0 requests, 5 seconds. Completed 0 requests of 4 estimated requests (0%). All tests completed.
Duration of Crawl Time: 1681.00 (seconds)
Duration of Test Phase: 3673.00 (seconds)
Total Scan Time: 5354.00 (seconds)

Total requests made: 29307
Average server response time: 0.19 seconds

Average browser load time: 0.18 seconds

150028 Cookies Collected (1)

150028 Cookies Collected

archibus.vodacom.co.za

Finding #	10510083	**Severity**	Information Gathered - Level 1
Unique #	5d8d15b9-7df4-4f6f-a5a3-432f1d202c08		
Group	Scan Diagnostics		
CWE	-	**Detection Date**	11 Feb 2024 21:02 GMT+0200
OWASP	-		
WASC	-		

Details

Threat
The cookies listed in the Results section were set by the web application during the crawl phase.

Impact
Cookies may potentially contain sensitive information about the user.

Note: Long scan duration can occur if a web application sets a large number of cookies (e.g., 25 cookies or more) and QIDs 150002, 150046, 150047, and 150048 are enabled.

Solution
Review cookie values to ensure they do not include sensitive information. If scan duration is excessive due to a large number of cookies, consider excluding QIDs 150002, 150046, 150047, and 150048.

Results

Total cookies: 4
visid_incap_2776849=FzwYQrB5SDmrEoE8GapjSPYZyWUAAAAAQUIPAAAAAACKSeVsUKW+PDQEFi62u5/P; HttpOnly; expires=Sun, 09-Feb-2025 22:21:11 GMT; domain=.vodacom.co.za; path=/ First set at URL: https://archibus.vodacom.co.za/
nlbi_2776849=2+b7ZdTvP3ssIFAPZU49BAAAAAATg/RB/1C/i+jo3xrjvYzk; domain=.vodacom.co.za; path=/ First set at URL: https://archibus.vodacom.co.za/
incap_ses_1687_2776849=lxYnX5C6qRDb7PgfvG1pF/YZyWUAAAAAg7Eia1/rhUGqMH+aaFiXQA==; domain=.vodacom.co.za; path=/ First set at URL: https://archibus.vodacom.co.za/
nlbi_2776849_2147483392=WoCbbZ/T0xODuuO8ZU49BAAAAAC4rTMSqcwSp5j8m2+NYJTV; domain=.vodacom.co.za; path=/ First set at URL: https://archibus.vodacom.co.za/

150097 HTTP Response Indicates Scan May Be Blocked (1)

150097 HTTP Response Indicates Scan May Be Blocked

archibus.vodacom.co.za

Finding #	10510086	**Severity**	Information Gathered - Level 1

WAS Web Application Report

Unique #	53587396-91e1-4c52-b15b-4b08e0af4930		
Group	Scan Diagnostics		
CWE	-	**Detection Date**	11 Feb 2024 21:02 GMT+0200
OWASP	-		
WASC	-		

Details

Threat

The scanner received an HTTP response from the target web site that contains a message indicating the scan has been blocked. This often occurs due to an intermediate security device such as a web application firewall (WAF), intrusion detection system (IDS), or intrusion prevention system (IPS).

Impact

If the scanner's IP or traffic has been blocked, then the results of the scan will be empty or incomplete because the web site could not be successfully crawled and tested.

Solution

Modify relevant security rules so that the WAS scans will not trigger alerts or be otherwise blocked. Additionally, review 150528 for additional HTTP 4XX Error Code responses found during the scanning.

Results

Uri: https://archibus.vodacom.co.za/_Incapsula_Resource?CWUDNSAI=23&xinfo=11-189604665-0%200NNN%20RT%2816840909218 55%202362%29%20q%280%20-1%20-1%200%29%20r%280%20-1%29%20B15%284%2C200%2C0%29%20U18&incident_id=764000300423775679-91206306729689 2811&edet=15&cinfo=04000000&rpinfo=0&mth=GET
Match: pan>

Powered by
Imperva

</body></html>

Uri: https://archibus.vodacom.co.za/_Incapsula_Resource?CWUDNSAI=23&xinfo=10-97597847-0%200NNN%20RT%2816919532713 88%207%29%20q%280%20-1%20-1%20-1%29%20r%280%20-1%29%20B15%284%2c200%2c0%29%20U18&incident_id=451001120180377263-459868152776563722&edet=15&cinfo=04000000&rpinfo=0&mth=GET
Match: pan>

Powered by
Imperva

</body></html>

Uri: https://archibus.vodacom.co.za/_Incapsula_Resource?CWUDNSAI=23&xinfo=11-217099708-0%200NNN%20RT%2816888929427 421%2010%29%20q%280%20-1%20-1%20-1%29%20r%280%20-1%29%20B15%284%2C200%2C0%29%20U18&incident_id=281000660478098624-104987613815852 6603&edet=15&cinfo=04000000&rpinfo=0&mth=GET
Match: pan>

Powered by
Imperva

</body></html>

Uri: https://archibus.vodacom.co.za/_Incapsula_Resource?CWUDNSAI=23&xinfo=12-68759309-0%200NNN%20RT%281686510514654%204%29%20q%280%20-1%20-1%20-1%29%20r%280%20-1%29%20B15%284%2c200%2c0%29%20U18&incident_id=767000350234861307-337740744850606284&edet=15&cinfo=04000000&rpinfo=0&mth=GET
Match: pan>

Powered by
Imperva

</body></html>

Uri: https://archibus.vodacom.co.za/_Incapsula_Resource?CWUDNSAI=23&xinfo=12-32525279-0%200NNN%20RT%281696791747727%209%29%20q%280%20-1%20-1%20-1%29%20r%280%20-1%29%20B15%284%2C200%2C0%29%20U18&incident_id=763001140096022537-164225543560699020&edet=15&cinfo=04000000&rpinfo=0&mth=GET
Match: pan>

Powered by
Imperva

</body></html>

Uri: https://archibus.vodacom.co.za/_Incapsula_Resource?CWUDNSAI=23&xinfo=10-42257572-0%200NNN%20RT%2816866510627231%202271%29%20q%280%20-1%20-1%200%29%20r%280%20-1%29%20B15%284%2C200%2C0%29%20U18&incident_id=767000350234861307-207301230861420746&edet=15&cinfo=04000000&rpinfo=0&mth=GET
Match: pan>

Powered by
Imperva

</body></html>

Uri: https://archibus.vodacom.co.za/_Incapsula_Resource?CWUDNSAI=23&xinfo=13-199918871-0%200NNN%20RT%2816999815731178%202650%29%20q%280%20-1%20-1%200%29%20r%280%20-1%29%20B15%284%2C200%2C0%29%20U18&incident_id=128000840526202745-103373459019321063 7&edet=15&cinfo=04000000&rpinfo=0&mth=GET
Match: pan>

Powered by
Imperva

</body></html>

Uri: https://archibus.vodacom.co.za/_Incapsula_Resource?CWUDNSAI=23&xinfo=11-93784308-0%200NNN%20RT%281702234859957%2012%29%20q%280%20-1%20-1%20-1%29%20r%280%20-1%29%20B15%284%2c200%2c0%29%20U18&incident_id=763001220427927261-490073197500898955&edet=15&cinfo=04000000&rpinfo=0&mth=GET

Match: pan>

Powered by
Imperva

</body></html>

Uri: https://archibus.vodacom.co.za/_Incapsula_Resource?CWUDNSAI=23&xinfo=11-61474434-0%200NNN%20RT%281686510627214%209%29%20q%280%20-1%20-1%20-1%29%20r%280%20-1%29%20B15%284%2C200%2C0%29%20U18&incident_id=767000350234861307-302640446746593483&edet=15&cinfo=04000000&rpinfo=0&mth=GET
Match: pan>

Powered by
Imperva

</body></html>

Uri: https://archibus.vodacom.co.za/_Incapsula_Resource?CWUDNSAI=23&xinfo=13-243380468-0%200NNN%20RT%281684090859136%203%29%20q%280%20-1%20-1%20-1%29%20r%280%20-1%29%20B15%284%2c200%2c0%29%20U18&incident_id=764000300423775679-117125871290836775 7&edet=15&cinfo=04000000&rpinfo=0&mth=GET
Match: pan>

Powered by
Imperva

</body></html>

Uri: https://archibus.vodacom.co.za/_Incapsula_Resource?CWUDNSAI=23&xinfo=12-217098056-0%200NNN%20RT%281684090921837%2011%29%20q%280%20-1%20-1%20-1%29%20r%280%20-1%29%20B15%284%2C200%2C0%29%20U18&incident_id=764000300423775679-1032818478005618572&edet=15&cinfo=04000000&rpinfo=0&mth=GET
Match: pan>

Powered by
Imperva

</body></html>

Uri: https://archibus.vodacom.co.za/_Incapsula_Resource?CWUDNSAI=23&xinfo=14-153614192-0%200NNN%20RT%281681066840725%203%29%20q%280%20-1%20-1%20-1%29%20r%280%20-1%29%20B15%284%2c200%2c0%29%20U18&incident_id=768000300342834631-735154962102749070&edet=15&cinfo=04000000&rpinfo=0&mth=GET
Match: pan>

Powered by

Imperva

</body></html>

Uri: https://archibus.vodacom.co.za/_Incapsula_Resource?CWUDNSAI=23&xinfo=14-34929213-0%200NNN%20RT%281696791682157%204%29%20q%280%20-1%20-1%20-1%29%20r%280%20-1%29%20B15%284%2c200%2c0%29%20U18&incident_id=763001140096022537-173542238158789774&edet=15&cinfo=04000000&rpinfo=0&mth=GET
Match: pan>

Powered by
Imperva

</body></html>

Uri: https://archibus.vodacom.co.za/_Incapsula_Resource?CWUDNSAI=23&xinfo=4-14899366-0%200NNN%20RT%281696791747744%202749%29%20q%280%20-1%20-1%200%29%20r%280%20-1%29%20B15%284%2C200%2C0%29%20U18&incident_id=763001140096022537-781033403776441644&edet=15&cinfo=04000000&rpinfo=0&mth=GET
Match: pan>

Powered by
Imperva

</body></html>

Uri: https://archibus.vodacom.co.za/_Incapsula_Resource?CWUDNSAI=23&xinfo=3-56251934-0%200NNN%20RT%281691953375915%209%29%20q%280%20-1%20-1%200%29%20r%280%20-1%29%20B15%284%2C200%2C0%29%20U18&incident_id=451001120180377263-267491121570192387&edet=15&cinfo=04000000&rpinfo=0&mth=GET
Match: pan>

Powered by
Imperva

</body></html>

Uri: https://archibus.vodacom.co.za/_Incapsula_Resource?CWUDNSAI=23&xinfo=2-25691562-0%200NNN%20RT%281694372513116%205%29%20q%280%20-1%20-1%20-1%29%20r%280%20-1%29%20B15%284%2c200%2c0%29%20U18&incident_id=451001150135587882-128340275738385602&edet=15&cinfo=04000000&rpinfo=0&mth=GET
Match: pan>

Powered by
Imperva

</body></html>

Uri: https://archibus.vodacom.co.za/_Incapsula_Resource?CWUDNSAI=23&xinfo=4-71886990-0%200NNN%20RT%281702234922706%202787%29%20q%280%20-1%20-1%201%29%20r

%280%20-1%29%20B15%284%2C200%2C0%29%20U18&incident_id=763001220427927261-377042573236838020&edet=15&cinfo=04000000&rpinfo=0&mth=GET
Match: pan>

Powered by
Imperva

</body></html>

Uri: https://archibus.vodacom.co.za/_Incapsula_Resource?CWUDNSAI=23&xinfo=5-13169156-0%200NNN%20RT%281705258980589%2010%29%20q%280%20-1%20-1%20-1%29%20r%280%20-1%29%20B15%284%2C200%2C0%29%20U18&incident_id=1687000060223901306-79686405253955973&edet=15&cinfo=04000000&rpinfo=0&mth=GET
Match: pan>

Powered by
Imperva

</body></html>

Uri: https://archibus.vodacom.co.za/_Incapsula_Resource?CWUDNSAI=23&xinfo=42-8036113-0%200NNN%20RT%281705258980606%202800%29%20q%280%20-1%20-1%202%29%20r%280%20-1%29%20B15%284%2C200%2C0%29%20U18&incident_id=1687000060223901306-46148676381770154&edet=15&cinfo=04000000&rpinfo=0&mth=GET
Match: pan>

Powered by
Imperva

</body></html>

Uri: https://archibus.vodacom.co.za/_Incapsula_Resource?CWUDNSAI=23&xinfo=5-90056699-0%200NNN%20RT%2816919533373089%209%29%20q%280%20-1%20-1%20-1%29%20r%280%20-1%29%20B15%284%2C200%2C0%29%20U18&incident_id=4510011201803772 63-41955995342308045 3&edet=15&cinfo=04000000&rpinfo=0&mth=GET
Match: pan>

Powered by
Imperva

</body></html>

Uri: https://archibus.vodacom.co.za/_Incapsula_Resource?CWUDNSAI=23&xinfo=5-94420317-0%200NNN%20RT%2816810668900 90%2010%29%20q%280%20-1%20-1%20-1%29%20r%281%20-1%29%20B15%284%2C200%2C0%29%20U18&incident_id=768000300342834631-44996192239825907 7&edet=15&cinfo=04000000&rpinfo=0&mth=GET
Match: pan>

Powered by
Imperva

</body></html>

Uri: https://archibus.vodacom.co.za/_Incapsula_Resource?CWUDNSAI=23&xinfo=5-88290743-0%200NNN%20RT%281702234922688%2010%29%20q%280%20-1%20-1%20-1%29%20r%280%20-1%29%20B15%284%2C200%2C0%29%20U18&incident_id=763001220427927261-45966233499524741&edet=15&cinfo=04000000&rpinfo=0&mth=GET
Match: pan>

Powered by
Imperva

</body></html>

Uri: https://archibus.vodacom.co.za/_Incapsula_Resource?CWUDNSAI=23&xinfo=5-94420320-0%200NNN%20RT%2816810668901 06%202879%29%20q%280%20-1%20-1%200%29%20r%280%20-1%29%20B15%284%2c200%2c0%29%20U18&incident_id=768000300342834631-449963447111649157&edet=15&cinfo=04000000&rpinfo=0&mth=GET
Match: pan>

Powered by
Imperva

</body></html>

Uri: https://archibus.vodacom.co.za/_Incapsula_Resource?CWUDNSAI=23&xinfo=5-94420320-0%200NNN%20RT%2816810668901 06%202879%29%20q%280%20-1%20-1%200%29%20r%280%20-1%29%20B15%284%2C200%2C0%29%20U18&incident_id=768000300342834631-449963447111649157&edet=15&cinfo=04000000&rpinfo=0&mth=GET
Match: pan>

Powered by
Imperva

</body></html>

Uri: https://archibus.vodacom.co.za/_Incapsula_Resource?CWUDNSAI=23&xinfo=57-13307322-0%200NNN%20RT%2817052588678 16%203%29%20q%280%20-1%20-1%20-1%29%20r%280%20-1%29%20B15%284%2c200%2c0%29%20U18&incident_id=168700006022390 1306-81567940232020409&edet=15&cinfo=04000000&rpinfo=0&mth=GET
Match: pan>

Powered by
Imperva

</body></html>

Uri: https://archibus.vodacom.co.za/_Incapsula_Resource?CWUDNSAI=23&xinfo=6-56552911-0%200NNN%20RT%2816998156722 06%205%29%20q%280%20-1%20-1%20-1%29%20r%280%20-1%29%20B15%284%2c200%2c0%29%20U18&incident_id=128000840526202745-294015529604093190&edet=15&cinfo=04000000&rpinfo=0&mth=GET
Match: pan>

Powered by
Imperva

</body></html>

Uri: https://archibus.vodacom.co.za/_Incapsula_Resource?CWUDNSAI=23&xinfo=8-86225779-0%200NNN%20RT%2816998157311 58%2013%29%20q%280%20-1%20-1%20-1%29%20r%280%20-1%29%20B15%284%2C200%2C0%29%20U18&incident_id=128000840526202745-446159613578974472&edet=15&cinfo=04000000&rpinfo=0&mth=GET
Match: pan>

Powered by
Imperva

</body></html>

Uri: https://archibus.vodacom.co.za/_Incapsula_Resource?CWUDNSAI=23&xinfo=8-36670336-0%200NNN%20RT%2816943725164 85%209%29%20q%280%20-1%20-1%20-1%29%20r%280%20-1%29%20B15%284%2C200%2C0%29%20U18&incident_id=451001150135587882-181277968159677640&edet=15&cinfo=04000000&rpinfo=0&mth=GET
Match: pan>

Powered by
Imperva

</body></html>

Uri: https://archibus.vodacom.co.za/_Incapsula_Resource?CWUDNSAI=23&xinfo=9-142966740-0%200NNN%20RT%2816888293 14974%202%29%20q%280%20-1%20-1%20-1%29%20r%280%20-1%29%20B15%284%2c200%2c0%29%20U18&incident_id=281000660478098624-6886809935665603 93&edet=15&cinfo=04000000&rpinfo=0&mth=GET
Match: pan>

Powered by
Imperva

</body></html>

Uri: https://archibus.vodacom.co.za/_Incapsula_Resource?CWUDNSAI=23&xinfo=9-63593046-0%200NNN%20RT%2816943725165 02%202831%29%20q%280%20-1%20-1%200%29%20r%280%20-1%29%20B15%284%2C200%2C0%29%20U18&incident_id=451001150135587882-313333098521763017&edet=15&cinfo=04000000&rpinfo=0&mth=GET
Match: pan>

Powered by
Imperva

</body></html>

Uri: https://archibus.vodacom.co.za/_Incapsula_Resource?CWUDNSAI=23&xinfo=9-142984614-0%200NNN%20RT%281688929427439%202760%29%20q%280%20-1%20-1%200%29%20r%281%20-1%29%20B15%284%2C200%2C0%29%20U18&incident_id=281000660478098624-688767335294111881&edet=15&cinfo=04000000&rpinfo=0&mth=GET
Match: pan>

Powered by
Imperva

</body></html>

Uri: https://archibus.vodacom.co.za/_Incapsula_Resource?CWUDNSAI=23&xinfo=9-84466755-0%200NNN%20RT%281691953378741%2023202%29%20q%280%20-1%20-1%200%29%20r%280%20-1%29%20B15%284%2C200%2C0%29%20U18&incident_id=451001120180377263-397119526690561033&edet=15&cinfo=04000000&rpinfo=0&mth=GET
Match: pan>

Powered by
Imperva

</body></html>

Uri: https://archibus.vodacom.co.za/_Incapsula_Resource?CWUDNSAI=23&xinfo=10-97597847-0%200NNN%20RT%281691953271388%207%29%20q%280%20-1%20-1%20-1%29%20r%280%20-1%29%20B15%284%2C200%2C0%29%20U18&incident_id=451001120180377263-459868152776563722&edet=15&cinfo=04000000&rpinfo=0&mth=GET
Match: pan>

Powered by
Imperva

</body></html>

150116 Server Authentication Found (1)

150116 Server Authentication Found

archibus.vodacom.co.za

Finding #	14173446	**Severity**	Information Gathered - Level 1
Unique #	63b6f8dc-8a2a-4d28-a741-3ceb02749210		
Group	Scan Diagnostics		
CWE	-	**Detection Date**	11 Feb 2024 21:02 GMT+0200
OWASP	-		
WASC	-		

Details

Threat
Server Authentication was found during the web application crawling.

Impact
N/A

Solution
N/A

Results

Server authentication found:
Url: https://archibus.vodacom.co.za/FPRWin/index.aspx
Type: unknown
Server authentication found:
Url: https://archibus.vodacom.co.za/FPRWin/index.aspx
Type: NTLM

150152 Forms Crawled (1)

150152 Forms Crawled — *archibus.vodacom.co.za*

Finding #	10510081	**Severity**	Information Gathered - Level 1
Unique #	ebad31c5-9a5f-4dd6-a46f-bdd2b2ab58f2		
Group	Scan Diagnostics		
CWE	-	**Detection Date**	11 Feb 2024 21:02 GMT+0200
OWASP	-		
WASC	-		

Details

Threat
The Results section lists the unique forms that were identified and submitted by the scanner. The forms listed in this QID do not include authentication forms (i.e. login forms), which are reported separately under QID 150115.

The scanner does a redundancy check on forms by inspecting the form fields. Forms determined to be the redundant based on identical form fields will not be tested. If desired, you can enable 'Include form action URI in form uniqueness calculation' in the WAS option profile to have the scanner also consider the form's action attribute in the redundancy check.

NOTE: Any regular expression specified under 'Redundant Links' are not applied to forms. Forms (unique or redundant) are not reported under QID 150140.

Impact
N/A

Solution
N/A

Results

Total internal forms seen (this count includes duplicate forms): 0

Crawled forms (Total: 0)
NOTE: This does not include authentication forms. Authentication forms are reported separately in QID 150115

WAS Web Application Report

150172 Requests Crawled (1)

150172 Requests Crawled

archibus.vodacom.co.za

Finding #	10510095	**Severity**	Information Gathered - Level 1
Unique #	c98fc1db-92f7-4acb-9f74-da75616a738b		
Group	Scan Diagnostics		
CWE	-	**Detection Date**	11 Feb 2024 21:02 GMT+0200
OWASP	-		
WASC	-		

Details

Threat
The QID reports list of requests crawled by the Web application scanner appear in the Results section.

Impact
N/A

Solution
N/A

Results

Number of crawled XHRs (XHRs, Fetch and External XHRs): 98

Fetch Requests: 98
Method POST URI https://archibus.vodacom.co.za/Leasure-the-deed-will-the-clipt-Angely-ands-Banq?d=archibus.vodacom.co.za (Count: 98)

150247 Web Server and Technologies Detected (1)

150247 Web Server and Technologies Detected

archibus.vodacom.co.za

Finding #	14173445	**Severity**	Information Gathered - Level 1
Unique #	5073eb66-bf90-4e67-9c6c-8094d2e49666		
Group	Scan Diagnostics		
CWE	CWE-200	**Detection Date**	11 Feb 2024 21:02 GMT+0200
OWASP	-		
WASC	-		

Details

Threat
Information disclosure is an application weakness in revealing sensitive data, such as technical details of the system or environment.

This check reports the various technologies used by the web application based on the information available in different components of the Request-Response.

Impact
An attacker may use sensitive data to exploit the target web application, its hosting network, or its users.

Solution
Ensure that your web servers do not reveal any sensitive information about your technology stack and system details

WAS Web Application Report

Please review the issues reported below:

Results

Number of technologies detected: 2
Technology name: Microsoft ASP.NET
Matched Components:
header match:
X-Powered-By:ASP.NET
Matched links: reporting only first 3 links
https://archibus.vodacom.co.za/FPRWin/
https://archibus.vodacom.co.za/FPRWin/index.aspx

Technology name: Microsoft IIS
Technology version: Microsoft IIS 10.0
Matched Components:
header match:
Server:Microsoft-IIS/10.0
Matched links: reporting only first 3 links
https://archibus.vodacom.co.za/FPRWin/
https://archibus.vodacom.co.za/FPRWin/index.aspx

150528 Server Returns HTTP 4XX Error Code During Scanning (1)

150528 Server Returns HTTP 4XX Error Code During Scanning — *archibus.vodacom.co.za*

Finding #	10510075	**Severity**	Information Gathered - Level 1
Unique #	84e5ceee-4cb0-432a-9ae3-065539c662c6		
Group	Scan Diagnostics		
CWE	-	**Detection Date**	11 Feb 2024 21:02 GMT+0200
OWASP	-		
WASC	-		

Details

Threat

During the WAS scan, links with HTTP 4xx response code were observed and these are listed in the Results section. The HTTP 4xx message indicates a client error. The list of supported 4xx response code are as below:

400 - Bad Request
401 - Unauthorized
403 - Forbidden
404 - Not Found
405 - Method Not Allowed
407 - Proxy Authentication Required
408 - Request Timeout
413 - Payload Too Large
414 - URI Too Long

Impact

The presence of a HTTP 4xx error during the crawl phase indicates that some problem exists on the website that will be encountered during normal usage of the Web application. Note WAS depends on responses to detect many vulnerabilities if the link does not respond with an expected response then any vulnerabilities present on such links may not be detected.

Solution

Review each link to determine why the client encountered an error while requesting the link. Additionally review and investigate the results of QID 150042 which lists 5xx errors, QID 150019 which lists unexpected response codes and QID 150097 which lists a potential blocked request.

WAS Web Application Report

Results

Number of links with 4xx response code: 36
(Only first 50 such links are listed)

401 https://archibus.vodacom.co.za/FPRWin/
401 https://archibus.vodacom.co.za/FPRWin/index.aspx
404 https://archibus.vodacom.co.za/_Incapsula_Resource?CWUDNSAI=23%22xinfo=10-42257572-0%200NNN%20RT%281686510627231%202271%29%20q%280%20-1%20-1%200%29%20r%280%20-1%29%20B15%284%2c200%2c0%29%20U18%22incident_id=767000350234861307-207301230861420746%22edet=15%22cinfo=04000000%22rpinfo=0%22mth=GET
404 https://archibus.vodacom.co.za/_Incapsula_Resource?CWUDNSAI=23%22xinfo=11-189604665-0%200NNN%20RT%281684090921855%202362%29%20q%280%20-1%20-1%200%29%20r%280%20-1%29%20B15%284%2c200%2c0%29%20U18%22incident_id=764000300423775679-912063067296892811%22edet=15%22cinfo=04000000%22rpinfo=0%22mth=GET
404 https://archibus.vodacom.co.za/_Incapsula_Resource?CWUDNSAI=23%22xinfo=13-199918871-0%200NNN%20RT%281699815731178%202650%29%20q%280%20-1%20-1%200%29%20r%280%20-1%29%20B15%284%2C200%2C0%29%20U18%22incident_id=128000840526202745-103373459019321063 7%22edet=15%22cinfo=04000000%22rpinfo=0%22mth=GET
404 https://archibus.vodacom.co.za/_Incapsula_Resource?CWUDNSAI=23%22xinfo=13-199918871-0%200NNN%20RT%281699815731178%202650%29%20q%280%20-1%20-1%200%29%20r%280%20-1%29%20B15%284%2c200%2c0%29%20U18%22incident_id=128000840526202745-103373459019321063 7%22edet=15%22cinfo=04000000%22rpinfo=0%22mth=GET
404 https://archibus.vodacom.co.za/_Incapsula_Resource?CWUDNSAI=23%22xinfo=3-56251934-0%200NNN%20RT%281691953375915%209%29%20q%280%20-1%20-1%200%29%20r%280%20-1%29%20B15%284%2C200%2C0%29%20U18%22incident_id=451001120180377263-267491121570192387%22edet=15%22cinfo=04000000%22rpinfo=0%22mth=GET
404 https://archibus.vodacom.co.za/_Incapsula_Resource?CWUDNSAI=23%22xinfo=3-56251934-0%200NNN%20RT%281691953375915%209%29%20q%280%20-1%20-1%200%29%20r%280%20-1%29%20B15%284%2c200%2c0%29%20U18%22incident_id=451001120180377263-267491121570192387%22edet=15%22cinfo=04000000%22rpinfo=0%22mth=GET
404 https://archibus.vodacom.co.za/_Incapsula_Resource?CWUDNSAI=23%22xinfo=4-14899366-0%200NNN%20RT%281696791747744%202749%29%20q%280%20-1%20-1%200%29%20r%280%20-1%29%20B15%284%2C200%2C0%29%20U18%22incident_id=763001140096022537-781033403776441 64%22edet=15%22cinfo=04000000%22rpinfo=0%22mth=GET
404 https://archibus.vodacom.co.za/_Incapsula_Resource?CWUDNSAI=23%22xinfo=4-14899366-0%200NNN%20RT%281696791747744%202749%29%20q%280%20-1%20-1%200%29%20r%280%20-1%29%20B15%284%2c200%2c0%29%20U18%22incident_id=763001140096022537-781033403776441 64%22edet=15%22cinfo=04000000%22rpinfo=0%22mth=GET
404 https://archibus.vodacom.co.za/_Incapsula_Resource?CWUDNSAI=23%22xinfo=4-71886990-0%200NNN%20RT%281702234922706%202787%29%20q%280%20-1%20-1%201%29%20r%280%20-1%29%20B15%284%2c200%2c0%29%20U18%22incident_id=763001220427927261-377042573236838020%22edet=15%22cinfo=04000000%22rpinfo=0%22mth=GET
404 https://archibus.vodacom.co.za/_Incapsula_Resource?CWUDNSAI=23%22xinfo=42-8036113-0%200NNN%20RT%281705258980606%202800%29%20q%280%20-1%20-1%202%29%20r%280%20-1%29%20B15%284%2c200%2c0%29%20U18%22incident_id=168700006022390 1306-46148676381770154%22edet=15%22cinfo=04000000%22rpinfo=0%22mth=GET
404 https://archibus.vodacom.co.za/_Incapsula_Resource?CWUDNSAI=23%22xinfo=9-142984614-0%200NNN%20RT%281688929427439%202760%29%20q%280%20-1%20-1%200%29%20r%281%20-1%29%20B15%284%2c200%2c0%29%20U18%22incident_id=281000660478098624-688767335294111881%22edet=15%22cinfo=04000000%22rpinfo=0%22mth=GET
404 https://archibus.vodacom.co.za/_Incapsula_Resource?CWUDNSAI=23%22xinfo=9-63593046-0%200NNN%20RT%281694372516502%202831%29%20q%280%20-1%20-1%200%29%20r%280%20-1%29%20B15%284%2c200%2c0%29%20U18%22incident_id=451001150135587882-313333098521763017%22edet=15%22cinfo=04000000%22rpinfo=0%22mth=GET
404 https://archibus.vodacom.co.za/_Incapsula_Resource?CWUDNSAI=23%22xinfo=9-84466755-0%200NNN%20RT%281691953378741%2023202%29%20q%280%20-1%20-1%200%29%20r%280%20-1%29%20B15%284%2c200%2c0%29%20U18%22incident_id=451001120180377263-397119526690561033%22edet=15%22cinfo=04000000%22rpinfo=0%22mth=GET
404 https://archibus.vodacom.co.za/docs/
404 https://archibus.vodacom.co.za/docs/RELEASE-NOTES.txt
404 https://archibus.vodacom.co.za/docs/api/
404 https://archibus.vodacom.co.za/docs/api/index.html
404 https://archibus.vodacom.co.za/docs/appdev/
404 https://archibus.vodacom.co.za/docs/changelog.html
404 https://archibus.vodacom.co.za/docs/cluster-howto.html
404 https://archibus.vodacom.co.za/docs/config/
404 https://archibus.vodacom.co.za/docs/deployer-howto.html
404 https://archibus.vodacom.co.za/docs/jndi-datasource-examples-howto.html
404 https://archibus.vodacom.co.za/docs/manager-howto.html
404 https://archibus.vodacom.co.za/docs/realm-howto.html
404 https://archibus.vodacom.co.za/docs/security-howto.html
404 https://archibus.vodacom.co.za/docs/setup.html
404 https://archibus.vodacom.co.za/examples/
404 https://archibus.vodacom.co.za/host-manager/
404 https://archibus.vodacom.co.za/host-manager/html
404 https://archibus.vodacom.co.za/manager/
404 https://archibus.vodacom.co.za/manager/html
404 https://archibus.vodacom.co.za/manager/status
404 https://archibus.vodacom.co.za/null

150546 First Link Crawled Response Code Information (1)

150546 First Link Crawled Response Code Information

archibus.vodacom.co.za

Finding #	10510085	**Severity**	Information Gathered - Level 1
Unique #	40e039b8-8764-4a1e-9420-3bba707a62de		
Group	Scan Diagnostics		
CWE	-	**Detection Date**	11 Feb 2024 21:02 GMT+0200
OWASP	-		
WASC	-		

Details

Threat

The Web server returned the following information from where the Web application scanning engine initiated. Information reported includes First Link Crawled,

response Code, response Header, and response Body (first 500 characters). The first link crawled is the "Web Application URL (or Swagger file URL)" set in the Web Application profile.

Impact

An erroneous response might be indicative of a problem in the Web server, or the scan configuration.

Solution

Review the information to check if this is in line with the expected scan configuration. Refer to the output of QIDs 150009, 150019, 150021, 150042 and 150528 (if present) for additional details.

Results

Base URI: https://archibus.vodacom.co.za/
Response Code: 302
Response Header:
Connection: Keep-Alive
Content-Length: 0
Content-Security-Policy-Report-Only: default-src 'self' 'unsafe-eval' 'unsafe-hashes' 'unsafe-inline' data: blob: ; form-action 'none' data: blob: ; report-uri /csp_report
Location: https://archibus.vodacom.co.za/FPRWin/index.aspx
Server: BigIP
X-CDN: Imperva
X-Iinfo: 56-11943627-11943785 NNNY CT(164 167 0) RT(1707678199943 3289) q(0 0 0 -1) r(1 1) U11
Set-Cookie: visid_incap_2776849=FzwYQrB5SDmrEoE8GapjSPYZyWUAAAAAQUIPAAAAAACKSeVsUKW+PDQEFi62u5/P; HttpOnly; expires=Sun, 09-Feb-2025 22:21:11 GMT; domain=.vodacom.co.za; path=/
Set-Cookie: nlbi_2776849=2+b7ZdTvP3ssIFAPZU49BAAAAAATg/RB/1C/i+jo3xrjvYzk; domain=.vodacom.co.za; path=/
Set-Cookie: incap_ses_1687_2776849=lxYnX5C6qRDb7PgfvG1pF/YZyWUAAAAAg7Eia1/rhUGqMH+aaFiXQA==; domain=.vodacom.co.za; path=/
Set-Cookie: nlbi_2776849_2147483392=WoCbbZ/T0xODuuO8ZU49BAAAAAC4rTMSqcwSp5j8m2+NYJTV; domain=.vodacom.co.za; path=/

Response Body:
<html><head></head><body></body></html>

150621 List of JavaScript Links (1)

150621 List of JavaScript Links

archibus.vodacom.co.za

Finding #	10510097	**Severity**	Information Gathered - Level 1
Unique #	4ed0023d-5d96-4f6f-a76a-06c29cee1a11		
Group	Scan Diagnostics		
CWE	-	**Detection Date**	11 Feb 2024 21:02 GMT+0200
OWASP	-		
WASC	-		

Details

Threat

This QID reports all the JavaScript links that are in-scope of this scan.

Impact

JavaScript links may pose security risks such as XSS, CSRF.

Solution

Verify JavaScript links are intentional and required for your web application.
Review any third party scripts that are hosted on your local server instead of using CDN.
Update all the JavaScript libraries with latest version as applicable.

Results

JavaScript Links were found while crawling.
Total Number of Links: 33
https://archibus.vodacom.co.za/Leasure-the-deed-will-the-clipt-Angely-ands-Banq
https://archibus.vodacom.co.za/_Incapsula_Resource?SWJIYLWA=719d34d31c8e3a6e6fffd425f7e032f3&ns=8&cb=1640283353

https://archibus.vodacom.co.za/_Incapsula_Resource?SWJIYLWA=719d34d31c8e3a6e6fffd425f7e032f3&ns=3&cb=1880170645
https://archibus.vodacom.co.za/Leasure-the-deed-will-the-clipt-Angely-ands-Banq?d=archibus.vodacom.co.za
https://archibus.vodacom.co.za/_Incapsula_Resource?SWJIYLWA=719d34d31c8e3a6e6fffd425f7e032f3&ns=21&cb=1906011217
https://archibus.vodacom.co.za/_Incapsula_Resource?SWJIYLWA=719d34d31c8e3a6e6fffd425f7e032f3%22ns=15%22cb=422869281
https://archibus.vodacom.co.za/_Incapsula_Resource?SWJIYLWA=719d34d31c8e3a6e6fffd425f7e032f3&ns=15&cb=422869281
https://archibus.vodacom.co.za/_Incapsula_Resource?SWJIYLWA=719d34d31c8e3a6e6fffd425f7e032f3&ns=30&cb=944403151
https://archibus.vodacom.co.za/_Incapsula_Resource?SWJIYLWA=719d34d31c8e3a6e6fffd425f7e032f3%22ns=23%22cb=1610054286
https://archibus.vodacom.co.za/_Incapsula_Resource?SWJIYLWA=719d34d31c8e3a6e6fffd425f7e032f3&ns=23&cb=1610054286
https://archibus.vodacom.co.za/_Incapsula_Resource?SWJIYLWA=719d34d31c8e3a6e6fffd425f7e032f3&ns=39&cb=1894920283
https://archibus.vodacom.co.za/_Incapsula_Resource?SWJIYLWA=719d34d31c8e3a6e6fffd425f7e032f3%22ns=32%22cb=939041622
https://archibus.vodacom.co.za/_Incapsula_Resource?SWJIYLWA=719d34d31c8e3a6e6fffd425f7e032f3&ns=32&cb=939041622
https://archibus.vodacom.co.za/_Incapsula_Resource?SWJIYLWA=719d34d31c8e3a6e6fffd425f7e032f3%22ns=41%22cb=1973595680
https://archibus.vodacom.co.za/_Incapsula_Resource?SWJIYLWA=719d34d31c8e3a6e6fffd425f7e032f3%22ns=44%22cb=974130296
https://archibus.vodacom.co.za/_Incapsula_Resource?SWJIYLWA=719d34d31c8e3a6e6fffd425f7e032f3%22ns=47%22cb=823359384
https://archibus.vodacom.co.za/_Incapsula_Resource?SWJIYLWA=719d34d31c8e3a6e6fffd425f7e032f3%22ns=62%22cb=48444639
https://archibus.vodacom.co.za/_Incapsula_Resource?SWJIYLWA=719d34d31c8e3a6e6fffd425f7e032f3%22ns=64%22cb=555618287
https://archibus.vodacom.co.za/_Incapsula_Resource?SWJIYLWA=719d34d31c8e3a6e6fffd425f7e032f3&ns=41&cb=1973595680
https://archibus.vodacom.co.za/_Incapsula_Resource?SWJIYLWA=719d34d31c8e3a6e6fffd425f7e032f3&ns=44&cb=974130296
https://archibus.vodacom.co.za/_Incapsula_Resource?SWJIYLWA=719d34d31c8e3a6e6fffd425f7e032f3&ns=47&cb=823359384
https://archibus.vodacom.co.za/_Incapsula_Resource?SWJIYLWA=719d34d31c8e3a6e6fffd425f7e032f3&ns=79&cb=394174316
https://archibus.vodacom.co.za/_Incapsula_Resource?SWJIYLWA=719d34d31c8e3a6e6fffd425f7e032f3&ns=82&cb=109097300
https://archibus.vodacom.co.za/_Incapsula_Resource?SWJIYLWA=719d34d31c8e3a6e6fffd425f7e032f3&ns=64&cb=555618287
https://archibus.vodacom.co.za/_Incapsula_Resource?SWJIYLWA=719d34d31c8e3a6e6fffd425f7e032f3&ns=62&cb=48444639
https://archibus.vodacom.co.za/_Incapsula_Resource?SWJIYLWA=719d34d31c8e3a6e6fffd425f7e032f3%22ns=63%22cb=837791161
https://archibus.vodacom.co.za/_Incapsula_Resource?SWJIYLWA=719d34d31c8e3a6e6fffd425f7e032f3%22ns=88%22cb=1271059637
https://archibus.vodacom.co.za/_Incapsula_Resource?SWJIYLWA=719d34d31c8e3a6e6fffd425f7e032f3&ns=63&cb=837791161
https://archibus.vodacom.co.za/_Incapsula_Resource?SWJIYLWA=719d34d31c8e3a6e6fffd425f7e032f3%22ns=90%22cb=212317304
https://archibus.vodacom.co.za/_Incapsula_Resource?SWJIYLWA=719d34d31c8e3a6e6fffd425f7e032f3&ns=88&cb=1271059637
https://archibus.vodacom.co.za/_Incapsula_Resource?SWJIYLWA=719d34d31c8e3a6e6fffd425f7e032f3&ns=90&cb=212317304
https://archibus.vodacom.co.za/_Incapsula_Resource?SWJIYLWA=719d34d31c8e3a6e6fffd425f7e032f3%22ns=89%22cb=463486056
https://archibus.vodacom.co.za/_Incapsula_Resource?SWJIYLWA=719d34d31c8e3a6e6fffd425f7e032f3&ns=89&cb=463486056

38116 SSL Server Information Retrieval (1)

38116 SSL Server Information Retrieval

archibus.vodacom.co.za

Finding #	10510107	**Severity**	Information Gathered - Level 1
Unique #	ca589730-6bd5-46ab-8f15-b12053744cf2		
Group	Scan Diagnostics		
CWE	-	**Detection Date**	11 Feb 2024 21:02 GMT+0200
OWASP	-		
WASC	-		

Details

Threat

The following is a list of supported SSL ciphers.

Note: If a cipher is included in this list it means that it was possible to establish a SSL connection using that cipher. There are some web servers setups that allow connections to be established using a LOW grade cipher, only to provide a web page stating that the URL is accessible only through a non-LOW grade cipher. In this case even though LOW grade cipher will be listed here QID 38140 will not be reported.

Impact

N/A

Solution

N/A

SSL Data

Flags	-
Protocol	tcp

WAS Web Application Report

Virtual Host	45.223.138.96
IP	45.223.138.96
Port	443
Result	#table cols="6" CIPHER KEY-EXCHANGE AUTHENTICATION MAC ENCRYPTION(KEY-STRENGTH) GRADE SSLv2_PROTOCOL_IS_DISABLED _ _ _ _ _ SSLv3_PROTOCOL_IS_DISABLED _ _ _ _ _ TLSv1_PROTOCOL_IS_DISABLED _ _ _ _ _ TLSv1.1_PROTOCOL_IS_DISABLED _ _ _ _ _ TLSv1.2_PROTOCOL_IS_ENABLED _ _ _ _ _ TLSv1.2 COMPRESSION_METHOD None _ _ _ AES128-SHA RSA RSA SHA1 AES(128) MEDIUM AES256-SH RSA RSA SHA1 AES(256) HIGH CAMELLIA128-SHA RSA RSA SHA1 Camellia(128) MEDIUM CAMELLIA256-SHA RSA RSA SHA1 Camellia(256) HIGH AES1 GCM-SHA256 RSA RSA AEAD AESGCM(128) MEDIUM AES256-GCM-SHA384 RSA RSA AEAD AESGCM(256) HIGH ECDHE-RSA-AES128-SHA ECDH RSA SHA1 AES(128) MEDIUM ECDHE-RSA-AES256-SHA ECDH RSA SHA1 AES(256) HIGH ECDHE-RSA-AES128-SHA256 ECDH RSA SHA256 AES(128) MEDI ECDHE-RSA-AES256-SHA384 ECDH RSA SHA384 AES(256) HIGH ECDHE-RSA-AES128-GCM-SHA256 ECDH RSA AEAD AESGCM(128) MEDIUM ECDHE RSA-AES256-GCM-SHA384 ECDH RSA AEAD AESGCM(256) HIGH ECDHE-RSA-CHACHA20-POLY1305 ECDH RSA AEAD CHACHA20/POLY1305(256) HI AES128-SHA256 RSA RSA SHA256 AES(128) MEDIUM AES256-SHA256 RSA RSA SHA256 AES(256) HIGH TLSv1.3_PROTOCOL_IS_ENABLED _ _ _ _ _ TLS13-AES-128-GCM-SHA256 N/A N/A AEAD AESGCM(128) MEDIUM TLS13-AES-256-GCM-SHA384 N/A N/A AEAD AESGCM(256) HIGH TLS13-CHACHA2 POLY1305-SHA256 N/A N/A AEAD CHACHA20/POLY1305(256) HIGH

Info List

Info #1

Ciphers

Name	Auth	Encryption	Grade	Key Exchange	Mac	Protocol
TLS13-AES-128-GCM-SHA256	N/A	AESGCM(128)	MEDIUM	N/A	AEAD	TLSv1.3
TLS13-AES-128-GCM-SHA256	N/A	AESGCM(256)	HIGH	N/A	AEAD	TLSv1.3
TLS13-AES-128-GCM-SHA256	N/A	CHACHA20/ POLY1305(256)	HIGH	N/A	AEAD	TLSv1.3

38291 SSL Session Caching Information (1)

38291 SSL Session Caching Information *archibus.vodacom.co.za*

Finding #	10510103	**Severity**	Information Gathered - Level 1
Unique #	a6bddbdf-f05d-42f3-a82e-22f9a7409910		
Group	Scan Diagnostics		
CWE	-	**Detection Date**	11 Feb 2024 21:02 GMT+0200
OWASP	-		
WASC	-		

Details

Threat

SSL session is a collection of security parameters that are negotiated by the SSL client and server for each SSL connection. SSL session caching is targeted to reduce the overhead of negotiations in recurring SSL connections. SSL sessions can be reused to resume an earlier connection or to establish multiple simultaneous connections. The client suggests an SSL session to be reused by identifying the session with a Session-ID during SSL handshake. If the server finds it appropriate to reuse the session, then they both proceed to secure communication with already known security parameters.

This test determines if SSL session caching is enabled on the host.

Impact

SSL session caching is part of the SSL and TLS protocols and is not a security threat. The result of this test is for informational purposes only.

Solution

N/A

SSL Data

Flags	-
Protocol	tcp
Virtual Host	45.223.138.96
IP	45.223.138.96
Port	443
Result	TLSv1.2 session caching is enabled on the target. TLSv1.3 session caching is enabled on the target.

Info List

Info #1

38597 Secure Sockets Layer/Transport Layer Security (SSL/TLS) Invalid Protocol Version Tolerance (1)

38597 Secure Sockets Layer/Transport Layer Security (SSL/TLS) Invalid Protocol Version Tolerance

archibus.vodacom.co.za

Finding #	10510106	**Severity**	Information Gathered - Level 1
Unique #	d566af07-3f5c-4ab5-a26a-0586447652dd		
Group	Scan Diagnostics		
CWE	-	**Detection Date**	11 Feb 2024 21:02 GMT+0200
OWASP	-		
WASC	-		

Details

Threat

SSL/TLS protocols have different version that can be supported by both the client and the server. This test attempts to send invalid protocol versions to the target in order to find out what is the target's behavior. The results section contains a table that indicates what was the target's response to each of our tests.

Impact

N/A

Solution

N/A

SSL Data

Flags	-
Protocol	tcp
Virtual Host	45.223.138.96
IP	45.223.138.96
Port	443
Result	#table cols=2 my_version target_version 0304 0303 0399 0303 0400 0303 0499 0303

Info List

Info #1

38600 SSL Certificate will expire within next six months (1)

38600 SSL Certificate will expire within next six months

archibus.vodacom.co.za

Finding #	10510100	**Severity**	Information Gathered - Level 1
Unique #	0420c328-300b-47c0-bd55-ef383b04435e		
Group	Scan Diagnostics		
CWE	-	**Detection Date**	11 Feb 2024 21:02 GMT+0200
OWASP	-		
WASC	-		

Details

Threat

Certificates are used for authentication purposes in different protocols such as SSL/TLS. Each certificate has a validity period outside of which it is supposed to be considered invalid. This QID is reported to inform that a certificate will expire within next six months. The advance notice can be helpful since obtaining a certificate can take some time.

Impact

Expired certificates can cause connection disruptions or compromise the integrity and privacy of the connections being protected by the certificates.

Solution

Contact the certificate authority that signed your certificate to arrange for a renewal.

SSL Data

Flags	-
Protocol	tcp
Virtual Host	45.223.138.96
IP	45.223.138.96
Port	443
Result	Certificate #0 CN=imperva.com The certificate will expire within six months: Jul 16 13:49:41 2024 GMT

Info List

Info #1

Certificate Fingerprint:5838E53F3C592C3FE144A59A3FF1EB4125C036D90CAEA8406E97249764E16408

38704 Secure Sockets Layer/Transport Layer Security (SSL/TLS) Key Exchange Methods (1)

38704 Secure Sockets Layer/Transport Layer Security (SSL/TLS) Key Exchange Methods

archibus.vodacom.co.za

Finding #	10510108	**Severity**	Information Gathered - Level 1
Unique #	b2e99e6d-a53b-4b80-b0f0-9ceec6b35380		
Group	Scan Diagnostics		
CWE	-	**Detection Date**	11 Feb 2024 21:02 GMT+0200
OWASP	-		
WASC	-		

Details

Threat
The following is a list of SSL/TLS key exchange methods supported by the server, along with their respective key sizes, strengths and ciphers.

Impact
N/A

Solution
N/A

SSL Data

Flags	-
Protocol	tcp
Virtual Host	45.223.138.96
IP	45.223.138.96
Port	443
Result	#table cols="6" NAME GROUP KEY-SIZE FORWARD-SECRET CLASSICAL-STRENGTH QUANTUM-STRENGTH TLSv1.2 _ _ _ _ _ RSA _ 2048 no 110 low ECDHE x25519 256 yes 128 low ECDHE secp256r1 256 yes 128 low ECDHE x448 448 yes 224 low ECDHE secp521r1 521 yes 260 low ECDHE secp384r1 384 yes 192 low TLSv1.3 _ _ _ _ _ ECDHE x25519 256 yes 128 low ECDHE secp256r1 256 yes 128 low ECDHE x448 448 yes 224 low ECDHE secp521r1 521 yes low ECDHE secp384r1 384 yes 192 low

Info List

Info #1

Kexs

Kex	Group	Protocol	Key Size		Classical	Quantum
RSA		TLSv1.2	2048	no	110	low
ECDHE		TLSv1.2	256	yes	128	low
ECDHE		TLSv1.2	256	yes	128	low
ECDHE		TLSv1.2	448	yes	224	low
ECDHE		TLSv1.2	521	yes	260	low
ECDHE		TLSv1.2	384	yes	192	low
ECDHE		TLSv1.3	256	yes	128	low
ECDHE		TLSv1.3	256	yes	128	low
ECDHE		TLSv1.3	448	yes	224	low
ECDHE		TLSv1.3	521	yes	260	low
ECDHE		TLSv1.3	384	yes	192	low

38706 Secure Sockets Layer/Transport Layer Security (SSL/TLS) Protocol Properties (1)

38706 Secure Sockets Layer/Transport Layer *archibus.vodacom.co.za*

WAS Web Application Report

Security (SSL/TLS) Protocol Properties

Finding #	10510109	**Severity**	Information Gathered - Level 1
Unique #	2f31a9f6-d188-439d-aed0-d6289c472a12		
Group	Scan Diagnostics		
CWE	-	**Detection Date**	11 Feb 2024 21:02 GMT+0200
OWASP	-		
WASC	-		

Details

Threat

The following is a list of detected SSL/TLS protocol properties.

Impact

Items include:

- Extended Master Secret: indicates whether the extended_master_secret extension is supported or required by the server. This extension enhances security and is recommended. Applicable to TLSv1, TLSv1.1, TLSv1.2, DTLSv1, DTLSv1.2
- Encrypt Then MAC: indicates whether the encrypt_then_mac extension is supported or required by the server. This extension enhances the security of non-AEAD ciphers and is recommended. Applicable to TLSv1, TLSv1.1, TLSv1.2, DTLSv1, DTLSv1.2
- Heartbeat: indicates whether the heartbeat extension is supported. It is not recommended to enable this, except for DTLS. Applicable to TLSv1, TLSv1.1, TLSv1.2, TLSv1.3, DTLSv1, DTLSv1.2
- Truncated HMAC: indicates whether the truncated_hmac extension is supported. This can degrade security and is not recommended. Applicable to TLSv1, TLSv1.1, TLSv1.2, DTLSv1, DTLSv1.2
- Cipher priority: indicates whether client, server or both determine the priority of ciphers. Having the server determine the priority is recommended. Applicable to SSLv3, TLSv1, TLSv1.1, TLSv1.2, TLSv1.3, DTLSv1, DTLSv1.2

Solution

N/A

SSL Data

Flags	-
Protocol	tcp
Virtual Host	45.223.138.96
IP	45.223.138.96
Port	443
Result	#table cols="2" NAME STATUS TLSv1.2 _ Extended_Master_Secret yes Encrypt_Then_MAC yes Heartbeat no Truncated_HMAC no Cipher_priority_controlled_server OCSP_stapling no SCT_extension no TLSv1.3 _ Heartbeat no Cipher_priority_controlled_by server OCSP_stapling no SCT_extension no

Info List

Info #1

Props

Name	Value	Protocol
Extended Master Secret	yes	TLSv1.2
Encrypt Then MAC	yes	TLSv1.2
Heartbeat	no	TLSv1.2
Truncated HMAC	no	TLSv1.2
Cipher priority controlled by	server	TLSv1.2
OCSP stapling	no	TLSv1.2
SCT extension	no	TLSv1.2
Heartbeat	no	TLSv1.3
Cipher priority controlled by	server	TLSv1.3
OCSP stapling	no	TLSv1.3
SCT extension	no	TLSv1.3

38717 Secure Sockets Layer (SSL) Certificate Online Certificate Status Protocol (OCSP) Information (1)

38717 Secure Sockets Layer (SSL) Certificate Online Certificate Status Protocol (OCSP) Information

archibus.vodacom.co.za

Finding #	10510101	**Severity**	Information Gathered - Level 1
Unique #	85a43264-f894-44ce-be18-b1eff9d32518		
Group	Scan Diagnostics		
CWE	-	**Detection Date**	11 Feb 2024 21:02 GMT+0200
OWASP	-		
WASC	-		

Details

Threat

OCSP (Online Certificate Status Protocol) is a protocol to determine the status of an SSL certificate, specifically whether a certificate has been revoked by the issuing certificate authority. SSL servers can provide the OCSP status of their certificate as part of the SSL/TLS handshake. This information is referred to as "Status Request" or "OCSP Stapling".

Impact

N/A

Solution

N/A

SSL Data

Flags	-
Protocol	tcp
Virtual Host	45.223.138.96
IP	45.223.138.96
Port	443
Result	Certificate #0 CN=archibus.vodacom.co.za,O=Vodafone_Group_Services_Limited,L=Newbury,C=GB OCSP status: good

Info List

Info #1

Certificate Fingerprint:0240E35B84FE2BCC96395D0CE97B03D511E35FC83F24034E9B73A3E054FA3A32

38718 Secure Sockets Layer (SSL) Certificate Transparency Information (1)

38718 Secure Sockets Layer (SSL) Certificate Transparency Information

archibus.vodacom.co.za

Finding #	10510102	**Severity**	Information Gathered - Level 1
Unique #	7dd9542d-bbaf-4d07-ab52-5f8ea57b674b		
Group	Scan Diagnostics		
CWE	-	**Detection Date**	11 Feb 2024 21:02 GMT+0200
OWASP	-		
WASC	-		

Details

Threat

SSL Certificate Transparency is an industry effort to improve visibility into the process of how certificate authorities issue certificates. It is designed to allow the owners of domain names to find all certificates that have been issued for their domains, and which certificate authorities have issued them. This is done by requiring certificate authorities to publish all issued certificates in public logs. TLS servers can then provide cryptographic evidence to TLS clients that the server certificate has been registered in public logs, thus providing some degree of confidence that the certificate is legitimate. Such cryptographic evidence is referred to as an "SCT Log Proof".

The information below lists all validated SCT Log Proofs for server certificates along with information about the public log, where available.

Impact

N/A

Solution

N/A

SSL Data

Flags	-
Protocol	tcp
Virtual Host	45.223.138.96
IP	45.223.138.96
Port	443
Result	#table cols="6" Source Validated Name URL ID Time Certificate_#0 _ CN=archibus.vodacom.co.za,O=Vodafone_Group_Services_Limited,L=Newbury,C=GB _ _

Certificate no (unknown) (unknown) eecdd064d5db1acec55cb79db4cd13a23287467cbcecdec351485946711fb59b Thu_01_Jan_1970_12:00:00_AM_GMT Certificate no (unknown) (unknown) 48b0e36bdaa647340fe56a02fa9d30eb1c5201cb56dd2c81d9bbbfab39d88473 Thu_01_Jan_1970_12:00:00_AM_GMT Certificate no (unknown) (unknown) dab6bf6b3fb5b6229f9bc2bb5c6be87091716cbb51848534bda43d3048d7fbab Thu_01_Jan_1970_12:00:00_AM_GMT Certificate_#0 _ CN=imperva.com _ _ _ Certificate no (unknown) (unknown) 76ff883f0ab6fb9551c261ccf587ba34b4a4cdbb29dc68420a9fe6674c5a3a74 Thu_01_Jan_1970_12:00:00_AM_GMT Certificate no (unknown) (unknown) 3b5377753e2db9804e8b305b06fe403b67d84fc3f4c7bd000d2d726fe1fad417 Thu_01_Jan_1970_12:00:00_AM_GMT Certificate no (unknown) (unknown) 48b0e36bdaa647340fe56a02fa9d30eb1c5201cb56dd2c81d9bbbfab39d88473 Thu_01_Jan_1970_12:00:00_AM_GMT

Info List

Info #1

Certificate Fingerprint:5838E53F3C592C3FE144A59A3FF1EB4125C036D90CAEA8406E97249764E16408

42350 TLS Secure Renegotiation Extension Support Information (1)

42350 TLS Secure Renegotiation Extension Support Information

archibus.vodacom.co.za

Finding #	10510105	**Severity**	Information Gathered - Level 1
Unique #	09c4589c-904f-4b9c-93be-c7bb6160dfe8		
Group	Scan Diagnostics		
CWE	-	**Detection Date**	11 Feb 2024 21:02 GMT+0200
OWASP	-		
WASC	-		

Details

Threat

Secure Socket Layer (SSL) and Transport Layer Security (TLS) renegotiation are vulnerable to an attack in which the attacker forms a TLS connection with the target server, injects content of his choice, and then splices in a new TLS connection from a client. The server treats the client's initial TLS handshake as a renegotiation and thus believes that the initial data transmitted by the attacker is from the same entity as the subsequent client data. TLS protocol was extended to cryptographically tierenegotiations to the TLS connections they are being performed over. This is referred to as TLS secure renegotiation extension. This detection determines whether the TLS secure renegotiation extension is supported by the server or not.

Impact

N/A

Solution

N/A

SSL Data

Flags	-
Protocol	tcp
Virtual Host	45.223.138.96
IP	45.223.138.96
Port	443
Result	TLS Secure Renegotiation Extension Status: supported.

Info List

Info #1

WAS Web Application Report

45038 Host Scan Time - Scanner (1)

45038 Host Scan Time - Scanner

archibus.vodacom.co.za

Finding #	10510084	**Severity**	Information Gathered - Level 1
Unique #	31e331d5-c7a1-46ce-9ebc-8bfa0d74cdd7		
Group	Scan Diagnostics		
CWE	-	**Detection Date**	11 Feb 2024 21:02 GMT+0200
OWASP	-		
WASC	-		

Details

Threat

The Host Scan Time is the period of time it takes the scanning engine to perform the vulnerability assessment of a single target host. The Host Scan Time for this host is reported in the Result section below.

The Host Scan Time does not have a direct correlation to the Duration time as displayed in the Report Summary section of a scan results report. The Duration is the period of time it takes the service to perform a scan task. The Duration includes the time it takes the service to scan all hosts, which may involve parallel scanning. It also includes the time it takes for a scanner appliance to pick up the scan task and transfer the results back to the service's Secure Operating Center. Further, when a scan task is distributed across multiple scanners, the Duration includes the time it takes to perform parallel host scanning on all scanners.

Impact

N/A

Solution

N/A

SSL Data

Flags	-
Protocol	-
Virtual Host	archibus.vodacom.co.za
IP	45.223.138.96
Port	-
Result	Scan duration: 5428 seconds Start time: Sun Feb 11 19:02:06 UTC 2024 End time: Sun Feb 11 20:32:34 UTC 2024

Info List

Info #1

6 DNS Host Name (1)

6 DNS Host Name

archibus.vodacom.co.za

Finding #	10510076	**Severity**	Information Gathered - Level 1
Unique #	e820ca32-47b4-4b37-9b67-7d0fc7dece42		
Group	Scan Diagnostics		
CWE	-	**Detection Date**	11 Feb 2024 21:02 GMT+0200
OWASP	-		
WASC	-		

Details

Threat
The fully qualified domain name of this host, if it was obtained from a DNS server, is displayed in the RESULT section.

Impact
N/A

Solution
N/A

SSL Data

Flags	-
Protocol	-
Virtual Host	45.223.138.96
IP	45.223.138.96
Port	-
Result	#table IP_address Host_name 45.223.138.96 No_registered_hostname

Info List

Info #1

86002 SSL Certificate - Information (1)

86002 SSL Certificate - Information *archibus.vodacom.co.za*

Finding #	10510099	**Severity**	Information Gathered - Level 1
Unique #	99014b5e-ab40-4727-8f31-0020a914b772		
Group	Scan Diagnostics		
CWE	-	**Detection Date**	11 Feb 2024 21:02 GMT+0200
OWASP	-		
WASC	-		

Details

Threat
SSL certificate information is provided in the Results section.

Impact
N/A

Solution
N/A

SSL Data

Flags	-

WAS Web Application Report

Protocol	tcp
Virtual Host	45.223.138.96
IP	45.223.138.96
Port	443
Result	#table cols="2" NAME VALUE (0)CERTIFICATE_0 _ (0)Version 3_(0x2) (0)Serial_Number _05:c6:21:a0:8b:cb:9d:a5:a9:50:27:34:56:03:00:0f_ (0)Signature_Algorithm sha256WithRSAEncryption (0)ISSUER_NAME _ countryName US _organizationName DigiCert_Inc _commonName DigiCert_SHA2_Secure_Server_CA (0)SUBJECT_NAME _ countryName GB _localityName Newbury _organizationName Vodafone_Group_Services_Limited _commonName archibus.vodacom.co.za (0)Valid_From Aug_11_00:00:00_2023_GMT (0)Valid_Till Aug_13_23:59:59_2024_GMT (0)Public_Key_Algorithm rsaEncryption (0)RSA_Public_Key (2048_bit) (0) _RSA_Public-Key:_(2048_bit) (0) _Modulus: (0) _00:95:50:81:28:a9:f1:89:02:18:87:b2:cb:e9:6f: (0) _6d:73:ee:e6 92:08:28:0b:71:fc:d7:01:34:86: (0) _43:c0:9c:74:c4:23:a9:cc:ef:d1:8d:61:25:27:3d: (0) _9f:f0:8b:65:be:57:1e:76:2e:e0:75:ca:9b:b1:8e: (0) _11:b5:5c:8b: 58:07:77:d1:15:e3:fc:f5:cc:31:6a: (0) _9c:01:42:f9:7a:02:61:6d:fe:33:2e:1f:85:9a:d3: (0) _e0:b5:89:ff:0b:38:1d:4f:9f:ee:6e:00:46:37:e1: (0) _bb:91:9d:cf: 76:14:43:c4:e2:33:21:f4:b4:5d:23: (0) _e7:86:d9:73:54:7c:7e:d4:5e:67:63:e1:22:d6:6a: (0) _2f:11:28:e3:0f:68:ef:1f:47:78:e4:98:55:af:af: (0) _54:08:91:ab:be: 24:21:78:59:f0:01:e6:70:b6:da: (0) _18:ae:48:65:e3:e8:2f:d1:bf:66:ca:1c:df:ce:01: (0) _14:51:20:51:5a:62:e4:83:c4:45:67:2a:e2:9d:a2: (0) _d8:1d:89:89:fd: 47:14:db:e6:8d:eb:53:55:89:5e: (0) _c0:70:b8:95:1a:7f:c7:00:b8:7a:3c:a9:be:03:cc: (0) _d8:21:8e:17:16:01:7e:9d:59:20:ef:aa:7d:8e:c4: (0) _3f:18:83:93:4f:ff:68:6e: 57:ae:ec:b7:8e:85:67: (0) _d9:3d (0) _Exponent:_65537_(0x10001) (0)X509v3_EXTENSIONS _ (0)X509v3_Authority_Key_Identifier _keyid:0F:80:61:1C: 82:31:61:D5:2F:28:E7:8D:46:38:B4:2C:E1:C6:D9:E2 (0)X509v3_Subject_Key_Identifier _57:7C:F8:D6:FD:53:52:92:12:99:03:79:B7:5D:F8:9E:18:CB:46:91 (0)X509v3_Subject_Alternative_Name _DNS:archibus.vodacom.co.za,_DNS:archibustest.vodacom.co.za,_DNS:archibusdev.vodacom.co.za (0)X509v3_Key_Usa critical (0) _Digital_Signature,_Key_Encipherment (0)X509v3_Extended_Key_Usage _TLS_Web_Server_Authentication,_TLS_Web_Client_Authentication (0)X509v3_CRL_Distribution_Points (0) _Full_Name: (0) _URI:http://crl3.digicert.com/DigicertSHA2SecureServerCA-1.crl (0) (0) _Full_Name: (0) _URI:http:// crl4.digicert.com/DigicertSHA2SecureServerCA-1.crl (0)X509v3_Certificate_Policies _Policy:_2.23.140.1.2.2 (0) _CPS:_http://www.digicert.com/CPS (0)Authority_Information_Access _OCSP_-_URI:http://ocsp.digicert.com (0) _CA_Issuers_-_URI:http://cacerts.digicert.com/DigiCertSHA2SecureServerCA-2.crt (0)X509v3_Basic_Constraints _CA:FALSE (0)CT_Precertificate_SCTs _Signed_Certificate_Timestamp: (0) _Version_:_v1_(0x0) (0) _Log_ID_:_EE:CD:D0:64:D5: 1A:CE:C5:5C:B7:9D:B4:CD:13:A2: (0) _32:87:46:7C:BC:EC:DE:C3:51:48:59:46:71:1F:B5:9B (0) _Timestamp_:_Aug_11_07:53:07.437_2023_GMT (0) _Extensions:_none (0) _Signature_:_ecdsa-with-SHA256 (0) _30:44:02:20:1C:66:C4:F7:06:8A:11:30:10:90:17:5F: (0) _2E:D9:7B:96:1F:80:16:0A:7E:39:A7:42:61: 24:79: (0) _60:64:13:59:02:20:7F:9C:0B:46:69:F1:D1:52:D5:DB: (0) _C2:90:5E:8D:07:36:59:42:44:A5:10:21:B5:D5:E2:2A: (0) _12:2B:BE:A3:79:F6 (0) _Signed_Certificate_Timestamp: (0) _Version_:_v1_(0x0) (0) _Log_ID_:_48:B0:E3:6B:DA:A6:47:34:0F:E5:6A:02:FA:9D:30:EB: (0) _1C:52:01:CB:56:DD:2C: 81:D9:BB:BF:AB:39:D8:84:73 (0) _Timestamp_:_Aug_11_07:53:07.439_2023_GMT (0) _Extensions:_none (0) _Signature_:_ecdsa-with-SHA256 (0) _30:45:02:20:70:D6:33:72:DD:4A:69:7A:A9:34:BF:72: (0) _71:E0:A8:79:E1:49:E0:B0:2A:45:E7:6F:FB:55:36:CA: (0) _D0:D2:17:8C:02:21:00:AB:FD:F7:70:AC:FF:I 7B:90: (0) _F5:3A:89:BD:F8:C1:4C:D5:1E:AD:03:36:F8:86:4B:26: (0) _15:CF:78:CD:28:BF:FB (0) _Signed_Certificate_Timestamp: (0) _Version_:_v1_(0x0) (0) _Log_ID_:_DA:B6:BF:6B:3F:B5:B6:22:9F:9B:C2:BB:5C:6B:E8:70: (0) _91:71:6C:BB:51:84:85:34:BD:A4:3D:30:48:D7:FB:AB (0) _Timestamp_:_Aug_11_07:53:07.365_2023_GMT (0) _Extensions:_none (0) _Signature_:_ecdsa-with-SHA256 (0) _30:45:02:21:00:82:73:A3:F7:55:A7:B7:B1:D7:19:6F: (0) _1A:B5:29:0A:86:B5:F9:BE:C1:C1:17:27:2C:EB:E0:2B: (0) _DE:71:4D:19:B3:02:20:5D:91:77:0D: 14:C5:43:6F:CB: (0) _FF:D3:70:A7:F6:65:18:08:E8:C6:5F:23:9B:3D:C3:84: (0) _59:64:8E:A0:2B:97:64 (0)Signature (256_octets) (0) ae: 83:b0:2d:c3:df:a7:d2:8a:b0:08:99:9e:28:c8:79 (0) 62:b8:3d:77:de:97:d6:b9:b5:1a:eb:90:a4:64:75:41 (0) 35:95:08:02:61:c7:8c:0c:8a:dd:6b:9b:81:69:9e:f0 (0) b0:df: 03:27:f1:6c:85:c1:04:86:f7:4d:2d:3a:07:f6 (0) 93:5c:f3:aa:66:51:ed:55:48:8e:50:e5:5f:f0:1c:03 (0) c2:83:ff:d2:c5:69:e0:dc:48:28:b3:c8:91:55:4b:a0 (0) 8a:fc:9f:8b: 26:9d:ce:3b:13:c0:d4:9a:a2:bf:a9:6f (0) d2:e7:77:5a:ef:5f:6f:e0:f5:bf:f6:56:58:41:98:ae (0) 0e:39:cf:11:32:16:67:0e:00:b5:ed:9b:54:02:e1:b9 (0) cf:0b: 38:81:13:b4:08:e6:d2:c0:3d:bc:7f:8a:5e:1d (0) f1:55:38:97:04:07:db:62:44:ba:15:df:50:3d:15:06 (0) b7:e5:c4:47:8f:55:a7:98:13:86:08:3c:9d:f9:d9:3a (0) 24:94:0f: 6b:a6:ae:87:3f:1d:71:c3:3f:90:75:c0:96 (0) 2d:dc:90:ee:e6:d3:30:47:68:56:26:2b:d8:18:28:3e (0) c0:11:8c:65:cc:84:dd:b1:f0:24:42:df:eb:d4:7f:b8 (0) 57:a9:21:f1:70:22:f0:7d:c2:25:09:14:04:92:20:40 (1)CERTIFICATE_1 _ (1)Version 3_(0x2) (1)Serial_Number _02:74:2e:aa:17:ca:8e:21:c7:17:bb:1f:fc:fd:0c:a0_ (1)Signature_Algorithm sha256WithRSAEncryption (1)ISSUER_NAME _ countryName US _organizationName DigiCert_Inc _organizationalUnitName www.digicert.com _commonName DigiCert_Global_Root_CA (1)SUBJECT_NAME _ countryName US _organizationName DigiCert_Inc _commonName DigiCert_SHA2_Secure_Server_CA (1)Valid_From Sep_23_00:00:00_2020_GMT (1)Valid_Till Sep_22_23:59:59_2030_GMT (1)Public_Key_Algorithm rsaEncryption (1)RSA_Public_Key (2048_bit) (1) _RSA_Public-Key:_(2048_bit) (1) _Modulus: (1) _00:dc:ae:58:90:4d:c1:c4:30:15:90:35:5b:6e:3c: (1) _82:15:f5:2c 5c:bd:e3:db:ff:71:43:fa:64:25:80: (1) _d4:ee:18:a2:4d:f0:66:d0:0a:73:6e:11:98:36:17: (1) _64:af:37:9d:fd:fa:41:84:af:c7:af:8c:fe:1a:73: (1) _4d:cf: 33:97:90:a2:96:87:53:83:2b:b9:a6:75:48: (1) _2d:1d:56:37:7b:da:31:32:1a:d7:ac:ab:06:f4:aa: (1) _5d:4b:b7:47:46:dd:2a:93:c3:90:2e:79:80:80:ef: (1) _13:04:6a: 14:3b:b5:9b:92:be:c2:07:65:4e:fc:da: (1) _fc:ff:7a:ae:dc:5c:7e:55:31:0c:e8:39:07:a4:d7: (1) _be:2f:d3:0b:6a:d2:b1:df:5f:fe:57:74:53:3b:35: (1) _80:dd:ae:8e: 44:98:b3:9f:0e:d3:da:e0:d7:f4:6b: (1) _29:ab:44:a7:4b:58:84:6d:92:4b:81:c3:da:73:8b: (1) _12:97:48:90:04:45:75:1a:dd:37:31:97:92:e8:cd: (1) _54:0d:3b:e4:c1:3f: 39:5e:2e:b8:f3:5c:7e:10:8e: (1) _86:41:00:8d:45:66:47:b0:a1:65:ce:a0:aa:29:09: (1) _4e:f3:97:eb:e8:2e:ab:0f:72:a7:30:0e:fa:c7:f4: (1) _fd:14:77:c3:a4:5b: 28:57:c2:b3:f9:82:fd:b7:45: (1) _58:9b (1) _Exponent:_65537_(0x10001) (1)X509v3_EXTENSIONS _ (1)X509v3_Subject_Key_Identifier _0F:80:61:1C: 82:31:61:D5:2F:28:E7:8D:46:38:B4:2C:E1:C6:D9:E2 (1)X509v3_Authority_Key_Identifier _keyid:03:DE:50:35:56:D1:4C:BB:66:F0:A3:E2:1B:1B:C3:97:B2:3D:D1:5 (1)X509v3_Key_Usage critical (1) _Digital_Signature,_Certificate_Sign,_CRL_Sign (1)X509v3_Extended_Key_Usage _TLS_Web_Server_Authentication,_TLS_Web_Client_Authentication (1)X509v3_Basic_Constraints critical (1) _CA:TRUE,_pathlen:0 (1)Authority_Information_Access _OCSP_-_URI:http://ocsp.digicert.com (1) _CA_Issuers_-_URI:http://cacerts.digicert.com/DigiCertGlobalRootCA.crt (1)X509v3_CRL_Distribution_Points (1) _Full_Name: (1) _URI:http://crl3.digicert.com/DigiCertGlobalRootCA.crl (1) (1) _Full_Name: (1) _URI:http://crl4.digicert.cor DigiCertGlobalRootCA.crl (1)X509v3_Certificate_Policies _Policy:_2.23.140.1.1 (1) _Policy:_2.23.140.1.2.1 (1) _Policy:_2.23.140.1.2.2 (1) _Policy:_2.23.140.1.2.3 (1)Signature (256_octets) (1) 77:31:1f:08:97:d7:12:9b:63:d2:11:65:08:a6:f6:65 (1) b9:b8:fa:92:03:cb:a1:7e:e1:c8:0d:8c:3e:b4:1b:91 (1) be:02:08:5e:9f:59:71:7b: 11:fd:e0:c0:e3:8f:59:d7 (1) a0:52:a1:d0:4b:54:d2:48:96:48:ef:77:e9:29:06:cb (1) 43:10:a0:2f:3c:16:8e:2d:fe:1e:55:3c:ec:c3:98:ee (1) 18:0d:23:e8:07:f5:b3:2d:c4:ab 57:73:5a:f6:1b:53 (1) ba:fb:1f:fa:bd:8c:d3:51:51:20:47:5e:ef:7f:98:ab (1) 17:42:ca:85:5c:9f:22:37:34:45:76:f2:43:5e:00:9e (1) 22:83:ac:df:af:d1:e6:c7:13:17:e9:a4:69:64:4c:80 (1) 67:ea:b6:a4:7f:8f:7d:e1:51:fa:9e:97:67:ea:69:2e (1) b3:90:a4:1c:15:c8:ac:cb:4f:29:ec:7a:5c:5d:9f:8a (1) b8:d4:0c:bb:94:ee:d0:bc:cb:b5:a5:1e:08:cf:c4:41 (1) 03:0d:bd:06:c3:a0:f4:c8:37:55:4a:f1:bf:e5:79:42 (1) 35:ab:41:98:ef:fc:13:39:c3:bb:5b:eb:ef:63:7c:80 (1) 9c:c8:49:46:70:6b:a0:82:50:3e:d0:04:b6:ca:25:c5 (1) c1:05:55:5f:f2:7c:2f:57:d1:af:95:6f:ac:6d:79:6b (2)CERTIFICATE_2 _ (2)Version 3_(0x2) (2)Serial_Number _08:3b:e0:56:90:42:46:b1:a1:75:6a:c9:59:91:c7:4a_ (2)Signature_Algorithm sha1WithRSAEncryption (2)ISSUER_NAME _ countryName US _organizationName DigiCert_Inc _organizationalUnitName www.digicert.com _commonName DigiCert_Global_Root_CA (2)SUBJECT_NAME _ countryName US _organizationName DigiCert_Inc _organizationalUnitName www.digicert.com _commonName DigiCert_Global_Root_CA (2)Valid_From Nov_10_00:00:00_2006_GMT (2)Valid_Till Nov_10_00:00:00_2031_GMT (2)Public_Key_Algorithm rsaEncryption (2)RSA_Public_Key (2048_bit) (2) _RSA_Public-Key:_(2048_bit) (2) _Modulus: (2) _00:e2:3b:e1:11:72:de:a8:a4:d3:a3:57:aa:50:a2: (2) _8f:0b:77:90:c9:a2:a5:ee:12:ce:96:5b:01:09:20: (2) _cc:01:93:a7:4e:30:b7:53:f7:43:c4:69:00:57:9d: (2) _e2:8d 22:dd:87:06:40:00:81:09:ce:ce:1b:83:bf: (2) _df:cd:3b:71:46:e2:d6:66:c7:05:b3:76:27:16:8f: (2) _7b:9e:1e:95:7d:ee:b7:48:a3:08:da:d6:af:7a:0c: (2) _39:06:65:7f:4a 5d:1f:bc:17:f8:ab:be:ee:28:d7: (2) _74:7f:7a:78:99:59:85:68:6e:5c:23:32:4b:bf:4e: (2) _c0:e8:5a:6d:e3:70:bf:77:10:bf:fc:01:f6:85:d9: (2) _a8:44:10:58:32:a9:75:18:d5:d1:a2:be:47:e2:27: (2) _6a:f4:9a:33:f8:49:08:60:8b:d4:5f:b4:3a:84:bf: (2) _a1:aa:4a:4c:7d:3e:cf:4f:5f:6c:76:5e:a0:4b:37: (2) _91:9e:dc 22:e6:6d:ce:14:1a:8e:6a:cb:fe:cd:b3: (2) _14:64:17:c7:5b:29:9e:32:bf:f2:ee:fa:d3:0b:42: (2) _d4:ab:b7:41:32:da:0c:d4:ef:f8:81:d5:bb:8d:58: (2) _3f:b5:1b:e8:49:28:a2:70:da:31:04:dd:f7:b2:16: (2) _f2:4c:0a:4e:07:a8:ed:4a:3d:5e:b5:7f:a3:90:c3: (2) _af:27 (2) _Exponent:_65537_(0x10001) (2)X509v3_EXTENSIONS _ (2)X509v3_Key_Usage critical (2) _Digital_Signature,_Certificate_Sign,_CRL_Sign (2)X509v3_Basic_Constraints critical (2) _CA:TRU (2)X509v3_Subject_Key_Identifier _03:DE:50:35:56:D1:4C:BB:66:F0:A3:E2:1B:1B:C3:97:B2:3D:D1:55 (2)X509v3_Authority_Key_Identifier _keyid:03:DE: 50:35:56:D1:4C:BB:66:F0:A3:E2:1B:1B:C3:97:B2:3D:D1:55 (2)Signature (256_octets) (2) cb:9c:37:aa:48:13:12:0a:fa:dd:44:9c:4f:52:b0:f4 (2) df:ae: 04:f5:79:79:08:a3:24:18:fc:4b:2b:84:c0:2d (2) b9:d5:c7:fe:f4:c1:1f:58:cb:b8:6d:9c:7a:74:e7:98 (2) 29:ab:11:b5:e3:70:a0:a1:cd:4c:88:99:93:8c:91:70 (2) e2:ab:0f:1c: 93:a9:ff:63:d5:e4:07:60:d3:a3:bf (2) 9d:5b:09:f1:d5:8e:e3:53:f4:8e:63:fa:3f:a7:db:b4 (2) 66:df:62:66:d6:d1:6e:41:8d:f2:2d:b5:ea:77:4a:9f (2) 9d:58:e2:2b: 59:c0:40:23:ed:2d:28:82:45:3e:79:54 (2) 92:26:98:e0:80:48:a8:37:ef:f0:d6:79:60:16:de:ac (2) e8:0e:cd:6e:ac:44:17:38:2f:49:da:e1:45:3e:2a:b9 (2) 36:53:cf:3a: 50:06:f7:2e:e8:c4:57:49:6c:61:21:18 (2) d5:04:ad:78:3c:2c:3a:80:6b:a7:eb:af:15:14:e9:d8 (2) 89:c1:b9:38:6c:e2:91:6c:8a:ff:64:b9:77:25:57:30 (2) c0:1b:

24:a3:e1:dc:e9:df:47:7c:b5:b4:24:08:05:30 (2) ec:2d:bd:0b:bf:45:bf:50:b9:a9:f3:eb:98:01:12:ad (2) c8:88:c6:98:34:5f:8d:0a:3c:c6:e9:d5:95:95:6d:de #table cols="2
NAME VALUE (0)CERTIFICATE_0 _ (0)Version 3_(0x2) (0)Serial_Number _01:8c:fc:40:a6:82:cc:44:37:35:84:76:9e:2f:e7:2a_ (0)Signature_Algorithm
sha256WithRSAEncryption (0)ISSUER_NAME _ countryName BE _organizationName GlobalSign_nv-sa _commonName
GlobalSign_Atlas_R3_DV_TLS_CA_2024_Q1 (0)SUBJECT_NAME _ commonName imperva.com (0)Valid_From Jan_18_13:49:41_2024_GMT (0)Valid_Till
Jul_16_13:49:41_2024_GMT (0)Public_Key_Algorithm rsaEncryption (0)RSA_Public_Key (2048_bit) (0) _RSA_Public-Key:_(2048_bit) (0) _Modulus: (0)
_00:b4:45:53:af:8c:d2:ca:21:2c:0c:a2:ea:0d:53: (0) _f4:17:ae:ad:ab:28:95:7d:5f:31:74:3d:7d:1a:3f: (0) _d6:c8:3c:cc:bc:b0:bb:ce:42:2f:cb:76:73:fb:3b: (0) _ef:44:8
4a:30:61:c0:c1:7f:6e:f9:03:e2:c8: (0) _0c:98:5a:b0:c4:00:47:93:dc:84:89:e4:50:91:09: (0) _39:a8:45:f1:97:61:4d:82:a4:4c:ce:d9:71:fd:01: (0) _e0:9f:
57:fa:c1:5a:da:ee:a1:6a:94:86:bd:20:93: (0) _e5:14:ed:60:6d:3e:db:a5:c2:cc:85:24:64:16:62: (0) _88:34:c1:12:7f:bc:f7:8c:8e:76:32:30:9d:dd:79: (0)
_7b:b0:4a:f6:38:f5:bc:ef:a8:99:cc:c3:15:ca:a9: (0) _0a:db:e1:64:71:fc:13:0b:6c:e8:4a:63:8e:f9:a8: (0) _3c:bb:ed:78:70:ab:3c:bd:27:e7:38:61:8a:2a:3b: (0)
_51:67:00:70:99:88:af:4b:ae:35:17:e0:83:02:34: (0) _f5:13:b1:96:16:41:50:60:99:41:39:fb:01:b0:4f: (0) _71:ad:20:53:dd:ad:8b:1d:aa:eb:06:40:bc:9c:08: (0) _9d:8
0d:bb:33:6d:f4:91:a7:80:0f:4e:c9:29:6b: (0) _0d:34:6a:14:a8:62:72:bd:a9:92:29:c5:29:ec:d8: (0) _1b:47 (0) _Exponent:_65537_(0x10001) (0)X509v3_EXTENSIO
_ (0)X509v3_Subject_Alternative_Name
_DNS:lending.vodacom.co.za,_DNS:hyperbook.vodacom.co.za,_DNS:journalist.vodacom.co.za,_DNS:de.c3dcrm.ppiam.vodacom.co.za,_DNS:nc.m2.ppret.voda
pwmicros.vodacom.co.za,_DNS:m2d.ret.vodacom.co.za,_DNS:kw3118.vod (0)
acom.co.za,_DNS:ciims.vodacom.co.za,_DNS:ifsfsmqa.vodacom.co.za,_DNS:cdn.mobucks.vodacom.co.za,_DNS:apix.vodacom.co.za,_DNS:nc.m2d.iam.vodac
ubuntu.vodacom.co.ls,_DNS:business.vodacom.co.za,_DNS:cc.m2d.ret.vodacom.co.za,_DNS:cc.m2.ppret.vodacom.co.za,_DNS:mobucks.sso. (0)
vodacom.co.za,_DNS:next.vodacom.co.za,_DNS:ifsfsm.vodacom.co.za,_DNS:cognosqa.sso.vodacom.co.za,_DNS:fr.m2.iam.vodacom.co.za,_DNS:nc.m2.iam.v
crm1.vodacom.co.za,_DNS:aplus-
dev.vodacom.co.za,_DNS:sorteos.mivodafoneapp.es,_DNS:login.ret.vodacom.co.za,_DNS:fr.m2d.ppret.vodacom.co.za,_DNS:etomrsso.vodacom.co.za,_DNS:fr
(0) nts.vodacom.co.za,_DNS:de.m2d.ppret.vodacom.co.za,_DNS:lendingdev.vodacom.co.za,_DNS:c3d-
crm.vodacom.co.za,_DNS:engageplatform.vodacom.co.za,_DNS:archibus.vodacom.co.za,_DNS:dwp.vodacom.co.za,_DNS:mobucks.ppent.vodacom.co.za,_DN
(0) _DNS:hcsadminapi.voicespend.vodacom.co.za,_DNS:m2.ppret.vodacom.co.za,_DNS:aplus-
qa.vodacom.co.za,_DNS:login.ent.vodacom.co.za,_DNS:de.c3dcrm.iam.vodacom.co.za,_DNS:public.tobicloud-
dev.vodafone.it,_DNS:consent.ppsso.vodacom.co.za,_DNS:*.to-
zi.com,_DNS:cc.m2d.iam.vodacom.co.za,_DNS:cc.m2.ppiam.vodacom.co.za,_DNS:login.thanos.co.za,_DNS:bcmapp.vodacom.co.za,_DNS:irsp.iam.vodacom.c
zi.com,_DNS:lendingqa.vodacom.co.za (0)X509v3_Key_Usage critical (0) _Digital_Signature,_Key_Encipherment (0)X509v3_Extended_Key_Usage
_TLS_Web_Server_Authentication,_TLS_Web_Client_Authentication (0)X509v3_Subject_Key_Identifier _2D:75:CE:D0:C6:36:E7:0A:AA:
02:47:60:D3:D3:07:25:22:48:58:17 (0)X509v3_Certificate_Policies _Policy:_2.23.140.1.2.1 (0) _Policy:_1.3.6.1.4.1.4146.10.1.3 (0) _CPS:_https://
www.globalsign.com/repository/ (0)X509v3_Basic_Constraints critical (0) _CA:FALSE (0)Authority_Information_Access _OCSP_-_URI:http://ocsp.globalsign.com
gsatlasr3dvtlsca2024q1 (0) _CA_Issuers_-_URI:http://secure.globalsign.com/cacert/gsatlasr3dvtlsca2024q1.crt (0)X509v3_Authority_Key_Identifier _keyid:
66:C0:C7:A3:9A:CD:FE:F3:EA:CE:4B:53:0B:61:5E:AF:33:05:B3:E1 (0)X509v3_CRL_Distribution_Points (0) _Full_Name: (0) _URI:http://crl.globalsign.com/ca/
gsatlasr3dvtlsca2024q1.crl (0)CT_Precertificate_SCTs _Signed_Certificate_Timestamp: (0) _Version_:_v1_(0x0) (0) _Log_ID_:_76:FF:88:3F:0A:B6:FB:
95:51:C2:61:CC:F5:87:BA:34: (0) _B4:A4:CD:BB:29:DC:68:42:0A:9F:E6:67:4C:5A:3A:74 (0) _Timestamp_:_Jan_18_13:50:14.915_2024_GMT (0)
_Extensions:_none (0) _Signature_:_ecdsa-with-SHA256 (0) _30:45:02:20:2A:87:69:07:90:39:65:94:75:77:FF:D0: (0) _36:EF:3A:28:9F:5B:44:AD:9D:34:CC:7F:
70:D1:22:2D: (0) _1D:BB:0B:09:02:21:00:A1:47:3B:73:1C:9B:16:4F:E7: (0) _21:3D:DA:DE:02:27:B5:7E:5D:D8:76:30:7E:97:0B:76: (0) _1A:51:40:FC:60:E3:B5 (0
_Signed_Certificate_Timestamp: (0) _Version_:_v1_(0x0) (0) _Log_ID_:_3B:53:77:75:3E:2D:B9:80:4E:8B:30:5B:06:FE:40:3B: (0) _67:D8:4F:C3:F4:C7:BD:00:0
72:6F:E1:FA:D4:17 (0) _Timestamp_:_Jan_18_13:50:15.031_2024_GMT (0) _Extensions:_none (0) _Signature_:_ecdsa-with-SHA256 (0)
_30:45:02:20:08:14:0B:B5:56:12:65:11:C8:E1:F3:AC: (0) _E8:FF:94:C8:5E:A0:2D:F7:7E:7B:13:6F:CA:64:CE:0E: (0) _18:F2:49:2C:02:21:00:E6:E6:BB:AF:89:7E
02:33:44: (0) _19:4C:6A:22:98:CD:E1:61:36:C0:FA:58:92:BB:E8:32: (0) _1C:E2:2F:11:B1:D3:D4 (0) _Signed_Certificate_Timestamp: (0) _Version_:_v1_(0x0) (0
_Log_ID_:_48:B0:E3:6B:DA:A6:47:34:0F:E5:6A:02:FA:9D:30:EB: (0) _1C:52:01:CB:56:DD:2C:81:D9:BB:BF:AB:39:D8:84:73 (0)
Timestamp:_Jan_18_13:50:15.338_2024_GMT (0) _Extensions:_none (0) _Signature_:_ecdsa-with-SHA256 (0) _30:45:02:21:00:83:84:EC:EF:2B:
59:53:02:10:C9:3C: (0) _0E:99:97:D8:50:35:1C:E5:9B:7F:46:01:8C:44:B2:F9: (0) _23:3E:9D:DB:CB:02:20:47:02:FE:EC:BD:B4:D5:1D:49: (0) _FF:17:9F:
01:12:47:EA:AA:E0:A8:72:E8:21:49:43:6D: (0) _CC:9F:4C:C2:42:16:73 (0)Signature (256_octets) (0) 7a:c3:19:8f:f8:f8:52:33:00:a5:aa:ef:21:09:db:48 (0)
a0:d3:62:75:cc:48:c4:2d:ed:84:27:95:28:cd:30:d4 (0) 11:2a:65:8b:83:ea:21:d8:1b:d2:4f:01:10:35:01:dd (0) e8:65:c1:a4:4a:64:06:46:24:a6:65:45:38:f9:6c:3b (0)
85:11:80:65:84:40:97:16:25:bf:c0:26:75:6d:6c:4c (0) a2:0d:ea:d4:16:f1:be:72:3b:da:a7:50:43:7d:22:18 (0) 3f:43:88:2e:9b:dd:53:9e:8f:28:88:84:d6:d9:be:77 (0) 2d
66:d1:f1:25:7a:ba:00:40:2f:11:67:98:81:ab (0) 04:21:79:dd:b0:6b:c1:f1:b5:f1:7e:89:72:fc:55:39 (0) 7c:3e:53:2d:c5:d3:fb:e3:43:b7:ae:06:f3:98:1a:41 (0) 8d:
5d:e2:80:84:dc:a5:7d:92:5f:d1:e5:1a:d2:c8:50 (0) 32:18:97:54:31:1b:70:1f:7d:5c:08:23:6f:e3:c9:9f (0) b8:81:c0:36:af:60:19:7a:8b:94:15:2b:9f:82:b4:81 (0)
43:2b:b0:c5:93:08:e5:23:41:d9:c4:60:0e:9c:00:d3 (0) 23:e3:ff:70:29:cb:3a:c7:16:dc:0a:e8:a3:f8:1c:8c (0) b1:f0:0d:cb:46:4d:96:41:d7:b2:44:c3:81:be:99:b9
(1)CERTIFICATE_1 _ (1)Version 3_(0x2) (1)Serial_Number _7f:b6:a0:ea:55:e2:8c:04:4c:95:2e:95:d6:34:9f:5c_ (1)Signature_Algorithm sha256WithRSAEncryptio
(1)ISSUER_NAME _ organizationalUnitName GlobalSign_Root_CA_-_R3 _organizationName GlobalSign _commonName GlobalSign (1)SUBJECT_NAME _
countryName BE _organizationName GlobalSign_nv-sa _commonName GlobalSign_Atlas_R3_DV_TLS_CA_2024_Q1 (1)Valid_From Oct_18_04:09:32_2023_G
(1)Valid_Till Oct_18_00:00:00_2025_GMT (1)Public_Key_Algorithm rsaEncryption (1)RSA_Public_Key (2048_bit) (1) _RSA_Public-Key:_(2048_bit) (1) _Modulu
(1) _00:94:46:a2:54:17:05:2e:68:70:09:bf:bd:79:95: (1) _0d:cb:1b:a8:dd:d7:5f:d6:a0:2a:a1:2f:47:45:4a: (1) _7a:6c:7b:f9:d0:3a:cf:3c:43:68:9e:2f:48:c7:82: (1) _55:
43:94:25:1b:f4:f0:f3:94:ab:01:86:f9:42: (1) _6b:b7:45:7d:fd:43:31:6f:dd:28:d8:84:48:0c:af: (1) _d0:b8:db:ab:af:7e:86:39:b3:18:5b:e2:bc:6c:d3: (1) _06:d1:12:86:22
8a:56:a6:4c:a8:56:81:3e:38: (1) _c6:99:66:44:3e:c9:70:58:38:fc:a9:bb:72:c2:83: (1) _b6:4c:c9:cc:a6:9c:4d:3b:29:a6:b3:a3:34:96:29: (1) _50:9c:12:b5:c9:a6:22:5d
18:d0:8c:ef:04:c2:43: (1) _8c:f7:98:8a:95:7c:74:6b:12:47:51:94:b9:9c:f9: (1) _04:be:ba:a9:ca:38:22:b2:40:ca:d8:44:db:e3:1a: (1)
_66:13:64:40:41:70:17:c4:cd:c5:a6:79:fd:93:13: (1) _22:d5:ab:7c:02:1b:16:c4:23:3f:a4:db:9c:53:aa: (1) _db:e2:ea:a2:6e:9f:4a:6d:b0:1d:84:3c:9d:fa:c2: (1)
_3a:bc:f6:43:4b:e4:6d:3a:6b:fe:6d:37:5a:00:f5: (1) _03:78:37:38:01:5e:ff:37:47:4e:54:c8:20:0a:9e: (1) _20:0f (1) _Exponent:_65537_(0x10001)
(1)X509v3_EXTENSIONS _ (1)X509v3_Key_Usage critical (1) _Digital_Signature,_Certificate_Sign,_CRL_Sign (1)X509v3_Extended_Key_Usage
_TLS_Web_Server_Authentication,_TLS_Web_Client_Authentication (1)X509v3_Basic_Constraints critical (1) _CA:TRUE,_pathlen:0
(1)X509v3_Subject_Key_Identifier _66:C0:C7:A3:9A:CD:FE:F3:EA:CE:4B:53:0B:61:5E:AF:33:05:B3:E1 (1)X509v3_Authority_Key_Identifier _keyid:8F:F0:4B:
7F:A8:2E:45:24:AE:4D:50:FA:63:9A:8B:DE:E2:DD:1B:BC (1)Authority_Information_Access _OCSP_-_URI:http://ocsp2.globalsign.com/rootr3 (1) _CA_Issuers_-
_URI:http://secure.globalsign.com/cacert/root-r3.crt (1)X509v3_CRL_Distribution_Points (1) _Full_Name: (1) _URI:http://crl.globalsign.com/root-r3.crl
(1)X509v3_Certificate_Policies _Policy:_2.23.140.1.2.1 (1) _Policy:_1.3.6.1.4.1.4146.10.1.3 (1)Signature (256_octets) (1) 1d:5a:11:af:98:37:f5:8f:fd:1c:c5:7c:
07:c5:69:fe (1) 00:b8:b2:af:a3:4c:86:88:27:0a:48:3d:17:34:0e:77 (1) 2f:8f:12:70:0d:47:2b:84:a4:8c:0b:e2:f1:64:fd:07 (1) c4:27:1e:7f:ee:e2:5d:0c:
33:33:f4:56:e0:33:f4:02 (1) 8e:be:be:19:75:88:b7:c5:c5:d0:7b:6a:da:a6:de:93 (1) c0:c6:c8:8c:be:f3:e4:96:ac:e5:9b:0d:9e:9c:27:e3 (1) b5:ae:63:03:97:ea:
89:28:a2:f1:35:c9:f1:67:86:d5 (1) 0c:44:8b:3a:8d:b2:ae:c2:fb:bc:bd:39:89:72:19:77 (1) 40:60:00:38:bb:c1:db:e2:0b:b9:e7:dc:da:3b:05:fc (1) bd:94:c2:9a:31:b7:bb:
2b:a7:6f:f5:41:33:38:aa (1) bc:d6:4f:d7:24:46:da:04:07:31:88:9a:1f:aa:e4:9d (1) c2:9e:30:4f:5f:dd:2a:d9:7d:8a:a9:13:fe:c6:23:ec (1) 17:5b:42:1a:6a:dc:ec:
09:d8:a6:2f:aa:cb:ae:4f:1a (1) 15:68:20:ee:c4:bf:dc:c8:ed:47:25:eb:c2:3f:de:b9 (1) aa:05:a8:4b:47:f2:81:d6:2b:18:0a:cd:1c:e7:b5:c6 (1) fa:93:26:67:5e:0a:af:
85:82:2e:e1:1f:5c:43:3c:b1

Info List

Info #1

Certificate Fingerprint:0152F86354FCA9525B280C233F7DA6CF8B5F2373C42644723226AE67238DB190

WAS Web Application Report

Security Weaknesses (14)

150210 Information Disclosure via Response Header (1)

150210 Information Disclosure via Response Header

archibus.vodacom.co.za

Finding #	14173444	**Severity**	Information Gathered - Level 3
Unique #	a0cfaa64-0dd3-45a7-9330-6fea65c374f9		
Group	Security Weaknesses		
CWE	CWE-16, CWE-201	**Detection Date**	11 Feb 2024 21:02 GMT+0200
OWASP	A5 Security Misconfiguration		
WASC	WASC-15 APPLICATION MISCONFIGURATION		

Details

Threat

HTTP response headers like 'Server', 'X-Powered-By', 'X-AspNetVersion', 'X-AspNetMvcVersion' could disclose information about the platform and technologies used by the website. The HTTP response include one or more such headers.

Impact

The headers can potentially be used by attackers for fingerprinting and launching attacks specific to the technologies and versions used by the web application. These response headers are not necessary for production sites and should be disabled.

Solution

Disable such response headers, remove them from the response, or make sure that the header value does not contain information which could be used to fingerprint the server-side components of the web application.

Results

One or more response headers disclosing information about the application platform were present on the following pages:
(Only first 50 such pages are reported)

GET https://archibus.vodacom.co.za/FPRWin/index.aspx response code: 401
Server: Microsoft-IIS/10.0
X-Powered-By: ASP.NET

GET https://archibus.vodacom.co.za/FPRWin/ response code: 401
Server: Microsoft-IIS/10.0
X-Powered-By: ASP.NET

150261 Subresource Integrity (SRI) Not Implemented (1)

150261 Subresource Integrity (SRI) Not Implemented

archibus.vodacom.co.za

Finding #	10510089	**Severity**	Information Gathered - Level 3
Unique #	ebf2acbf-048e-45b5-be93-3259ca47dc72		
Group	Security Weaknesses		
CWE	CWE-693	**Detection Date**	11 Feb 2024 21:02 GMT+0200
OWASP	-		
WASC	-		

Details

Threat

The integrity attribute is missing in script and/or link elements. Subresource Integrity (SRI) is a standard browser security feature that verifies the value of the integrity attribute in

Impact

Absence of SRI checks means it is impossible to verify that the third-party resources are delivered without any unexpected manipulation.

Solution

All script and link elements that load external content should include the integrity attribute to ensure that the content is trustworthy.

More information:
Subresource Integrity article by Mozilla
OWASP Third-Party JavaScript Management Cheat Sheet

Results

Externally loaded Javascript and CSS resources without integrity checks:

Parent link : https://archibus.vodacom.co.za/_Incapsula_Resource?CWUDNSAI=23&xinfo=10-97597847-0%200NNN%20RT%281691953271388%207%29%20q%280%20-1%20-1%20-1%29%20r%280%20-1%29%20B15%284%2c200%2c0%29%20U18&incident_id=451001120180377263-459868152776563722&edet=15&cinfo=04000000&rpinfo=0&mth=GET
Found following resource links without integrity checks (only first 10 links are reported)
https://fonts.googleapis.com/css2?family=Inter:wght@300;400;500;700&display=swap

Parent link : https://archibus.vodacom.co.za/_Incapsula_Resource?CWUDNSAI=23&xinfo=11-189604665-0%200NNN%20RT%2816840909921855%202362%29%20q%280%20-1%20-1%200%29%20r
%280%20-1%29%20B15%284%2C200%2C0%29%20U18&incident_id=764000300423775679-912063067296892811&edet=15&cinfo=04000000&rpinfo=0&mth=GET
Found following resource links without integrity checks (only first 10 links are reported)
https://fonts.googleapis.com/css2?family=Inter:wght@300;400;500;700&display=swap

Parent link : https://archibus.vodacom.co.za/_Incapsula_Resource?CWUDNSAI=23&xinfo=11-217099708-0%200NNN%20RT%2816888929427421%2010%29%20q%280%20-1%20-1%20-1%29%20r
%280%20-1%29%20B15%284%2C200%2C0%29%20U18&incident_id=2810006604780986 24-1049876138158526603&edet=15&cinfo=04000000&rpinfo=0&mth=GET
Found following resource links without integrity checks (only first 10 links are reported)
https://fonts.googleapis.com/css2?family=Inter:wght@300;400;500;700&display=swap

Parent link : https://archibus.vodacom.co.za/_Incapsula_Resource?CWUDNSAI=23&xinfo=10-42257572-0%200NNN%20RT%2816865106272 31%202271%29%20q%280%20-1%20-1%200%29%20r
%280%20-1%29%20B15%284%2C200%2C0%29%20U18&incident_id=767000350234861307-207301230861420746&edet=15&cinfo=04000000&rpinfo=0&mth=GET
Found following resource links without integrity checks (only first 10 links are reported)
https://fonts.googleapis.com/css2?family=Inter:wght@300;400;500;700&display=swap

Parent link : https://archibus.vodacom.co.za/_Incapsula_Resource?CWUDNSAI=23&xinfo=12-32525279-0%200NNN%20RT%2816967917477 27%209%29%20q%280%20-1%20-1%20-1%29%20r%280%20-1%29%20B15%284%2C200%2C0%29%20U18&incident_id=763001140096022537-164225543560699020&edet=15&cinfo=04000000&rpinfo=0&mth=GET
Found following resource links without integrity checks (only first 10 links are reported)
https://fonts.googleapis.com/css2?family=Inter:wght@300;400;500;700&display=swap

Parent link : https://archibus.vodacom.co.za/_Incapsula_Resource?CWUDNSAI=23&xinfo=12-68759309-0%200NNN%20RT%2816865105146 54%204%29%20q%280%20-1%20-1%20-1%29%20r%280%20-1%29%20B15%284%2c200%2c0%29%20U18&incident_id=767000350234861307-337740744850606284&edet=15&cinfo=04000000&rpinfo=0&mth=GET
Found following resource links without integrity checks (only first 10 links are reported)
https://fonts.googleapis.com/css2?family=Inter:wght@300;400;500;700&display=swap

Parent link : https://archibus.vodacom.co.za/_Incapsula_Resource?CWUDNSAI=23&xinfo=13-199918871-0%200NNN%20RT%2816999815731178%202650%29%20q%280%20-1%20-1%200%29%20r
%280%20-1%29%20B15%284%2C200%2C0%29%20U18&incident_id=128000840526202745-103373459019321 0637&edet=15&cinfo=04000000&rpinfo=0&mth=GET
Found following resource links without integrity checks (only first 10 links are reported)
https://fonts.googleapis.com/css2?family=Inter:wght@300;400;500;700&display=swap

Parent link : https://archibus.vodacom.co.za/_Incapsula_Resource?CWUDNSAI=23&xinfo=11-61474434-0%200NNN%20RT%2816865106272 14%209%29%20q%280%20-1%20-1%20-1%29%20r%280%20-1%29%20B15%284%2C200%2C0%29%20U18&incident_id=767000350234861307-302640446746593483&edet=15&cinfo=04000000&rpinfo=0&mth=GET
Found following resource links without integrity checks (only first 10 links are reported)
https://fonts.googleapis.com/css2?family=Inter:wght@300;400;500;700&display=swap

Parent link : https://archibus.vodacom.co.za/_Incapsula_Resource?CWUDNSAI=23&xinfo=11-93784308-0%200NNN%20RT%281702234859957%2012%29%20q%280%20-1%20-1%20-1%29%20r%280%20-1%29%20B15%284%2c200%2c0%29%20U18&incident_id=763001220427927261-490073197500898955&edet=15&cinfo=04000000&rpinfo=0&mth=GET
Found following resource links without integrity checks (only first 10 links are reported)
https://fonts.googleapis.com/css2?family=Inter:wght@300;400;500;700&display=swap

Parent link : https://archibus.vodacom.co.za/_Incapsula_Resource?CWUDNSAI=23&xinfo=12-217098056-0%200NNN%20RT%2816840909218 37%2011%29%20q%280%20-1%20-1%20-1%29%20r
%280%20-1%29%20B15%284%2C200%2C0%29%20U18&incident_id=764000300423775679-103281847800561 8572&edet=15&cinfo=04000000&rpinfo=0&mth=GET
Found following resource links without integrity checks (only first 10 links are reported)
https://fonts.googleapis.com/css2?family=Inter:wght@300;400;500;700&display=swap

Parent link : https://archibus.vodacom.co.za/_Incapsula_Resource?CWUDNSAI=23&xinfo=14-153614192-0%200NNN%20RT%2816810668407 25%203%29%20q%280%20-1%20-1%20-1%29%20r%280%20-1%29%20B15%284%2c200%2c0%29%20U18&incident_id=768000300342834631-735154962102749070&edet=15&cinfo=04000000&rpinfo=0&mth=GET
Found following resource links without integrity checks (only first 10 links are reported)
https://fonts.googleapis.com/css2?family=Inter:wght@300;400;500;700&display=swap

Parent link : https://archibus.vodacom.co.za/_Incapsula_Resource?CWUDNSAI=23&xinfo=13-243380468-0%200NNN%20RT%2816840908591 36%203%29%20q%280%20-1%20-1%20-1%29%20r

%280%20-1%29%20B15%284%2c200%2c0%29%20U18&incident_id=764000300423775679-117125871290836775 7&edet=15&cinfo=04000000&rpinfo=0&mth=GET
Found following resource links without integrity checks (only first 10 links are reported)
https://fonts.googleapis.com/css2?family=Inter:wght@300;400;500;700&display=swap

Parent link : https://archibus.vodacom.co.za/_Incapsula_Resource?CWUDNSAI=23&xinfo=14-34929213-0%200NNN%20RT%281696791682157%204%29%20q%280%20-1%20-1%20-1%29%20r%280%20-1%29%20B15%284%2c200%2c0%29%20U18&incident_id=763001140096022537-173542238158789774&edet=15&cinfo=04000000&rpinfo=0&mth=GET
Found following resource links without integrity checks (only first 10 links are reported)
https://fonts.googleapis.com/css2?family=Inter:wght@300;400;500;700&display=swap

Parent link : https://archibus.vodacom.co.za/_Incapsula_Resource?CWUDNSAI=23&xinfo=3-56251934-0%200NNN%20RT%281691953375915%209%29%20q%280%20-1%20-1%200%29%20r%280%20-1%29%20B15%284%2C200%2C0%29%20U18&incident_id=451001120180377263-267491121570192387&edet=15&cinfo=04000000&rpinfo=0&mth=GET
Found following resource links without integrity checks (only first 10 links are reported)
https://fonts.googleapis.com/css2?family=Inter:wght@300;400;500;700&display=swap

Parent link : https://archibus.vodacom.co.za/_Incapsula_Resource?CWUDNSAI=23&xinfo=2-25691562-0%200NNN%20RT%281694372513116%205%29%20q%280%20-1%20-1%20-1%29%20r%280%20-1%29%20B15%284%2c200%2c0%29%20U18&incident_id=451001150135587882-128340275738385602&edet=15&cinfo=04000000&rpinfo=0&mth=GET
Found following resource links without integrity checks (only first 10 links are reported)
https://fonts.googleapis.com/css2?family=Inter:wght@300;400;500;700&display=swap

Parent link : https://archibus.vodacom.co.za/_Incapsula_Resource?CWUDNSAI=23&xinfo=4-14899366-0%200NNN%20RT%281696791747744%202749%29%20q%280%20-1%20-1%200%29%20r%280%20-1%29%20B15%284%2C200%2C0%29%20U18&incident_id=763001140096022537-781033403776441 64&edet=15&cinfo=04000000&rpinfo=0&mth=GET
Found following resource links without integrity checks (only first 10 links are reported)
https://fonts.googleapis.com/css2?family=Inter:wght@300;400;500;700&display=swap

Parent link : https://archibus.vodacom.co.za/_Incapsula_Resource?CWUDNSAI=23&xinfo=42-8036113-0%200NNN%20RT%281705258980606%202800%29%20q%280%20-1%20-1%202%29%20r%280%20-1%29%20B15%284%2C200%2C0%29%20U18&incident_id=1687000060223901306-46148676381770154&edet=15&cinfo=04000000&rpinfo=0&mth=GET
Found following resource links without integrity checks (only first 10 links are reported)
https://fonts.googleapis.com/css2?family=Inter:wght@300;400;500;700&display=swap

Parent link : https://archibus.vodacom.co.za/_Incapsula_Resource?CWUDNSAI=23&xinfo=5-13169156-0%200NNN%20RT%281705258980589%2010%29%20q%280%20-1%20-1%20-1%29%20r%280%20-1%29%20B15%284%2C200%2C0%29%20U18&incident_id=1687000060223901306-7968640525395597 3&edet=15&cinfo=04000000&rpinfo=0&mth=GET
Found following resource links without integrity checks (only first 10 links are reported)
https://fonts.googleapis.com/css2?family=Inter:wght@300;400;500;700&display=swap

Parent link : https://archibus.vodacom.co.za/_Incapsula_Resource?CWUDNSAI=23&xinfo=4-71886990-0%200NNN%20RT%281702234922706%202787%29%20q%280%20-1%20-1%201%29%20r%280%20-1%29%20B15%284%2C200%2C0%29%20U18&incident_id=763001220427927261-377042573236838020&edet=15&cinfo=04000000&rpinfo=0&mth=GET
Found following resource links without integrity checks (only first 10 links are reported)
https://fonts.googleapis.com/css2?family=Inter:wght@300;400;500;700&display=swap

Parent link : https://archibus.vodacom.co.za/_Incapsula_Resource?CWUDNSAI=23&xinfo=5-88290743-0%200NNN%20RT%281702234922688%2010%29%20q%280%20-1%20-1%20-1%29%20r%280%20-1%29%20B15%284%2C200%2C0%29%20U18&incident_id=763001220427927261-459666233499524741&edet=15&cinfo=04000000&rpinfo=0&mth=GET
Found following resource links without integrity checks (only first 10 links are reported)
https://fonts.googleapis.com/css2?family=Inter:wght@300;400;500;700&display=swap
Please check there may be more pages with subresource links without integrity checks.

150202 Missing header: X-Content-Type-Options (1)

150202 Missing header: X-Content-Type-Options

archibus.vodacom.co.za

Finding #	10510091	**Severity**	Information Gathered - Level 2
Unique #	d805a19c-f606-4344-ae6e-84cfe47c9e69		
Group	Security Weaknesses		
CWE	CWE-16, CWE-1032	**Detection Date**	11 Feb 2024 21:02 GMT+0200
OWASP	A5 Security Misconfiguration		
WASC	WASC-15 APPLICATION MISCONFIGURATION		

Details

Threat

The X-Content-Type-Options response header is not present. WAS reports missing X-Content-Type-Options header on each crawled link for both static and dynamic responses. The scanner performs the check not only on 200 responses but 4xx and 5xx responses as well. It's also possible the QID will be reported on directory-level links.

Impact

All web browsers employ a content-sniffing algorithm that inspects the contents of HTTP responses and also occasionally overrides the MIME type provided by the server. If X-Content-Type-Options header is not present, browsers can potentially be tricked into treating non-HTML response as HTML. An attacker can then potentially leverage the functionality to perform a cross-site scripting (XSS) attack. This specific case is known as a Content-Sniffing XSS (CS-XSS) attack.

Solution

It is recommended to disable browser content sniffing by adding the X-Content-Type-Options header to the HTTP response with a value of 'nosniff'. Also, ensure that the 'Content-Type' header is set correctly on responses.

Results

X-Content-Type-Options: Header missing
Response headers on link: GET https://archibus.vodacom.co.za/Leasure-the-deed-will-the-clipt-Angely-ands-Banq response code: 200
Cache-Control: max-age=47, public
Content-Encoding: gzip
Content-Length: 77738
Content-Security-Policy-Report-Only: default-src 'self' 'unsafe-eval' 'unsafe-hashes' 'unsafe-inline' data: blob: ; form-action 'none' data: blob: ; report-uri /csp_report
Content-Type: text/javascript
Date: Sun, 11 Feb 2024 19:03:30 GMT
Etag: "4df2a20d"
Expires: Sun, 11 Feb 2024 19:04:17 GMT
X-CDN: Imperva
X-Iinfo: 56-11943627-0 0CNN RT(1707678199943 10992) q(0 -1 -1 -1) r(0 -1)
Set-Cookie: visid_incap_2776849=FzwYQrB5SDmrEoE8GapjSPYZyWUAAAAAQUIPAAAAAACKSeVsUKW+PDQEFi62u5/P; HttpOnly; expires=Sun, 09-Feb-2025 22:21:11 GMT; domain=.vodacom.co.za; path=/
Set-Cookie: nlbi_2776849=2+b7ZdTvP3ssIFAPZU49BAAAAAATg/RB/1C/i+jo3xrjvYzk; domain=.vodacom.co.za; path=/
Set-Cookie: incap_ses_1687_2776849=lxYnX5C6qRDb7PgfvG1pF/YZyWUAAAAg7Eia1/rhUGqMH+aaFiXQA==; domain=.vodacom.co.za; path=/
Set-Cookie: nlbi_2776849_2147483392=WoCbbZ/T0xODuuO8ZU49BAAAAAC4rTMSqcwSp5j8m2+NYJTV; domain=.vodacom.co.za; path=/

Header missing on the following link(s):
(Only first 50 such pages are listed)

GET https://archibus.vodacom.co.za/Leasure-the-deed-will-the-clipt-Angely-ands-Banq response code: 200
GET https://archibus.vodacom.co.za/favicon.ico response code: 200
GET https://archibus.vodacom.co.za/tomcat.css response code: 200
GET https://archibus.vodacom.co.za/docs/ response code: 404
GET https://archibus.vodacom.co.za/docs/config/ response code: 404
GET https://archibus.vodacom.co.za/examples/ response code: 404
GET https://archibus.vodacom.co.za/docs/cluster-howto.html response code: 404
GET https://archibus.vodacom.co.za/docs/security-howto.html response code: 404
GET https://archibus.vodacom.co.za/docs/manager-howto.html response code: 404
GET https://archibus.vodacom.co.za/manager/status response code: 404
GET https://archibus.vodacom.co.za/manager/html response code: 404
GET https://archibus.vodacom.co.za/host-manager/html response code: 404
GET https://archibus.vodacom.co.za/docs/realm-howto.html response code: 404
GET https://archibus.vodacom.co.za/docs/setup.html response code: 404
GET https://archibus.vodacom.co.za/docs/appdev/ response code: 404
GET https://archibus.vodacom.co.za/docs/changelog.html response code: 404
GET https://archibus.vodacom.co.za/docs/jndi-datasource-examples-howto.html response code: 404
GET https://archibus.vodacom.co.za/docs/RELEASE-NOTES.txt response code: 404
GET https://archibus.vodacom.co.za/_Incapsula_Resource?SWJIYLWA=719d34d31c8e3a6e6fffd425f7e032f3&ns=8&cb=1640283353 response code: 200
GET https://archibus.vodacom.co.za/docs/deployer-howto.html response code: 404
GET https://archibus.vodacom.co.za/docs/api/index.html response code: 404
GET https://archibus.vodacom.co.za/FPRWin/index.aspx response code: 401
GET https://archibus.vodacom.co.za/_Incapsula_Resource?SWJIYLWA=719d34d31c8e3a6e6fffd425f7e032f3&ns=3&cb=1880170645 response code: 200
GET https://archibus.vodacom.co.za/Leasure-the-deed-will-the-clipt-Angely-ands-Banq?d=archibus.vodacom.co.za response code: 200
GET https://archibus.vodacom.co.za/_Incapsula_Resource?SWKMTFSR=1&e=0.5329770916436014 response code: 200
GET https://archibus.vodacom.co.za/_Incapsula_Resource?SWJIYLWA=719d34d31c8e3a6e6fffd425f7e032f3&ns=21&cb=1906011217 response code: 200
GET https://archibus.vodacom.co.za/_Incapsula_Resource?SWJIYLWA=719d34d31c8e3a6e6fffd425f7e032f3%22ns=15%22cb=422869281 response code: 200
GET https://archibus.vodacom.co.za/_Incapsula_Resource?SWJIYLWA=719d34d31c8e3a6e6fffd425f7e032f3&ns=15&cb=422869281 response code: 200
GET https://archibus.vodacom.co.za/_Incapsula_Resource?SWKMTFSR=1&e=0.7902679497011122 response code: 200
GET https://archibus.vodacom.co.za/_Incapsula_Resource?SWJIYLWA=719d34d31c8e3a6e6fffd425f7e032f3&ns=30&cb=944403151 response code: 200
GET https://archibus.vodacom.co.za/_Incapsula_Resource?SWJIYLWA=719d34d31c8e3a6e6fffd425f7e032f3%22ns=23%22cb=1610054286 response code: 200
GET https://archibus.vodacom.co.za/_Incapsula_Resource?SWJIYLWA=719d34d31c8e3a6e6fffd425f7e032f3&ns=23&cb=1610054286 response code: 200
GET https://archibus.vodacom.co.za/_Incapsula_Resource?SWKMTFSR=1&e=0.6767940789579447 response code: 200
GET https://archibus.vodacom.co.za/_Incapsula_Resource?SWJIYLWA=719d34d31c8e3a6e6fffd425f7e032f3&ns=39&cb=1894920283 response code: 200
GET https://archibus.vodacom.co.za/_Incapsula_Resource?SWJIYLWA=719d34d31c8e3a6e6fffd425f7e032f3%22ns=32%22cb=939041622 response code: 200
GET https://archibus.vodacom.co.za/_Incapsula_Resource?SWJIYLWA=719d34d31c8e3a6e6fffd425f7e032f3&ns=32&cb=939041622 response code: 200
GET https://archibus.vodacom.co.za/_Incapsula_Resource?SWJIYLWA=719d34d31c8e3a6e6fffd425f7e032f3%22ns=41%22cb=1973595680 response code: 200
GET https://archibus.vodacom.co.za/_Incapsula_Resource?SWKMTFSR=1&e=0.8560383602618578 response code: 200
GET https://archibus.vodacom.co.za/_Incapsula_Resource?SWKMTFSR=1&e=0.4472103130471645 response code: 200
GET https://archibus.vodacom.co.za/_Incapsula_Resource?SWJIYLWA=719d34d31c8e3a6e6fffd425f7e032f3%22ns=44%22cb=974130296 response code: 200
GET https://archibus.vodacom.co.za/_Incapsula_Resource?SWKMTFSR=1&e=0.913395824408842 response code: 200
GET https://archibus.vodacom.co.za/_Incapsula_Resource?SWKMTFSR=1&e=0.4981508946970825 response code: 200
GET https://archibus.vodacom.co.za/_Incapsula_Resource?SWJIYLWA=719d34d31c8e3a6e6fffd425f7e032f3%22ns=47%22cb=823359384 response code: 200
GET https://archibus.vodacom.co.za/host-manager/ response code: 404
GET https://archibus.vodacom.co.za/manager/ response code: 404
GET https://archibus.vodacom.co.za/_Incapsula_Resource?SWJIYLWA=719d34d31c8e3a6e6fffd425f7e032f3%22ns=62%22cb=48444639 response code: 200
GET https://archibus.vodacom.co.za/_Incapsula_Resource?SWKMTFSR=1&e=0.7227896506086273 response code: 200
GET https://archibus.vodacom.co.za/_Incapsula_Resource?SWJIYLWA=719d34d31c8e3a6e6fffd425f7e032f3%22ns=64%22cb=555618287 response code: 200
GET https://archibus.vodacom.co.za/docs/api/ response code: 404
GET https://archibus.vodacom.co.za/FPRWin/ response code: 401

150206 Content-Security-Policy Not Implemented (1)

WAS Web Application Report

150206 Content-Security-Policy Not Implemented

archibus.vodacom.co.za

Finding #	10510094	**Severity**	Information Gathered - Level 2
Unique #	20bc8e77-5371-41ba-a681-4bace511fd31		
Group	Security Weaknesses		
CWE	CWE-16, CWE-1032	**Detection Date**	11 Feb 2024 21:02 GMT+0200
OWASP	A5 Security Misconfiguration		
WASC	WASC-15 APPLICATION MISCONFIGURATION		

Details

Threat

No Content-Security-Policy (CSP) is specified for the page. WAS checks for the missing CSP on all static and dynamic pages. It checks for CSP in the response headers (Content-Security-Policy, X-Content-Security-Policy or X-Webkit-CSP) and in response body (http-equiv="Content-Security-Policy" meta tag).

HTTP 4xx and 5xx responses can also be susceptible to attacks such as XSS. For better security it's important to set appropriate CSP policies on 4xx and 5xx responses as well.

Impact

Content-Security Policy is a defense mechanism that can significantly reduce the risk and impact of XSS attacks in modern browsers. The CSP specification provides a set of content restrictions for web resources and a mechanism for transmitting the policy from a server to a client where the policy is enforced. When a Content Security Policy is specified, a number of default behaviors in user agents are changed; specifically inline content and JavaScript eval constructs are not interpreted without additional directives. In short, CSP allows you to create a whitelist of sources of the trusted content. The CSP policy instructs the browser to only render resources from those whitelisted sources. Even though an attacker can find a security vulnerability in the application through which to inject script, the script won't match the whitelisted sources defined in the CSP policy, and therefore will not be executed.

The absence of Content Security Policy in the response will allow the attacker to exploit vulnerabilities as the protection provided by the browser is not at all leveraged by the Web application. If secure CSP configuration is not implemented, browsers will not be able to block content-injection attacks such as Cross-Site Scripting and Clickjacking.

Solution

Appropriate CSP policies help prevent content-injection attacks such as cross-site scripting (XSS) and clickjacking. It's recommended to add secure CSP policies as a part of a defense-in-depth approach for securing web applications.

References:
- https://cheatsheetseries.owasp.org/cheatsheets/Content_Security_Policy_Cheat_Sheet.html
- https://developers.google.com/web/fundamentals/security/csp/

Results

Content-Security-Policy: Header missing
Response headers on link: GET https://archibus.vodacom.co.za/Leasure-the-deed-will-the-clipt-Angely-ands-Banq response code: 200
Cache-Control: max-age=47, public
Content-Encoding: gzip
Content-Length: 77738
Content-Security-Policy-Report-Only: default-src 'self' 'unsafe-eval' 'unsafe-hashes' 'unsafe-inline' data: blob: ; form-action 'none' data: blob: ; report-uri /csp_report
Content-Type: text/javascript
Date: Sun, 11 Feb 2024 19:03:30 GMT
Etag: "4df2a20d"
Expires: Sun, 11 Feb 2024 19:04:17 GMT
X-CDN: Imperva
X-Iinfo: 56-11943627-0 0CNN RT(1707678199943 10992) q(0 -1 -1 -1) r(0 -1)
Set-Cookie: visid_incap_2776849=FzwYQrB5SDmrEoE8GapjSPYZyWUAAAAAQUIPAAAAAACKSeVsUKW+PDQEFi62u5/P; HttpOnly; expires=Sun, 09-Feb-2025 22:21:11 GMT; domain=.vodacom.co.za; path=/
Set-Cookie: nlbi_2776849=2+b7ZdTvP3ssIFAPZU49BAAAAAATg/RB/1C/i+jo3xrjvYzk; domain=.vodacom.co.za; path=/
Set-Cookie: incap_ses_1687_2776849=lxYnX5C6qRDb7PgfvG1pF/YZyWUAAAAAg7Eia1/rhUGqMH+aaFiXQA==; domain=.vodacom.co.za; path=/
Set-Cookie: nlbi_2776849_2147483392=WoCbbZ/T0xODuuO8ZU49BAAAAAC4rTMSqcwSp5j8m2+NYJTV; domain=.vodacom.co.za; path=/

Header missing, but Content-Security-Policy-Report-Only header found. It allows for testing different directives to determine how the current policy can be trimmed or modified to create the most restrictive policy possible, however still allowing all required resources. CSP header missing on the link: GET https://archibus.vodacom.co.za/Leasure-the-deed-will-the-clipt-Angely-ands-Banq response code: 200

Content-Security-Policy: Header missing, but Content-Security-Policy-Report-Only header found. It allows for testing different directives to determine how the current policy can be trimmed or

modified to create the most restrictive policy possible, however still allowing all required resources. CSP header missing on the link: GET https://archibus.vodacom.co.za/favicon.ico response code: 200

Content-Security-Policy: Header missing, but Content-Security-Policy-Report-Only header found. It allows for testing different directives to determine how the current policy can be trimmed or modified to create the most restrictive policy possible, however still allowing all required resources. CSP header missing on the link: GET https://archibus.vodacom.co.za/tomcat.css response code: 200

Content-Security-Policy: Header missing, but Content-Security-Policy-Report-Only header found. It allows for testing different directives to determine how the current policy can be trimmed or modified to create the most restrictive policy possible, however still allowing all required resources. CSP header missing on the link: GET https://archibus.vodacom.co.za/docs/ response code: 404

Content-Security-Policy: Header missing, but Content-Security-Policy-Report-Only header found. It allows for testing different directives to determine how the current policy can be trimmed or modified to create the most restrictive policy possible, however still allowing all required resources. CSP header missing on the link: GET https://archibus.vodacom.co.za/docs/config/ response code: 404

Content-Security-Policy: Header missing, but Content-Security-Policy-Report-Only header found. It allows for testing different directives to determine how the current policy can be trimmed or modified to create the most restrictive policy possible, however still allowing all required resources. CSP header missing on the link: GET https://archibus.vodacom.co.za/examples/ response code: 404

Content-Security-Policy: Header missing, but Content-Security-Policy-Report-Only header found. It allows for testing different directives to determine how the current policy can be trimmed or modified to create the most restrictive policy possible, however still allowing all required resources. CSP header missing on the link: GET https://archibus.vodacom.co.za/docs/cluster-howto.html response code: 404

Content-Security-Policy: Header missing, but Content-Security-Policy-Report-Only header found. It allows for testing different directives to determine how the current policy can be trimmed or modified to create the most restrictive policy possible, however still allowing all required resources. CSP header missing on the link: GET https://archibus.vodacom.co.za/docs/security-howto.html response code: 404

Content-Security-Policy: Header missing, but Content-Security-Policy-Report-Only header found. It allows for testing different directives to determine how the current policy can be trimmed or modified to create the most restrictive policy possible, however still allowing all required resources. CSP header missing on the link: GET https://archibus.vodacom.co.za/docs/manager-howto.html response code: 404

Content-Security-Policy: Header missing, but Content-Security-Policy-Report-Only header found. It allows for testing different directives to determine how the current policy can be trimmed or modified to create the most restrictive policy possible, however still allowing all required resources. CSP header missing on the link: GET https://archibus.vodacom.co.za/manager/status response code: 404

Content-Security-Policy: Header missing, but Content-Security-Policy-Report-Only header found. It allows for testing different directives to determine how the current policy can be trimmed or modified to create the most restrictive policy possible, however still allowing all required resources. CSP header missing on the link: GET https://archibus.vodacom.co.za/manager/html response code: 404

Content-Security-Policy: Header missing, but Content-Security-Policy-Report-Only header found. It allows for testing different directives to determine how the current policy can be trimmed or modified to create the most restrictive policy possible, however still allowing all required resources. CSP header missing on the link: GET https://archibus.vodacom.co.za/host-manager/html response code: 404

Content-Security-Policy: Header missing, but Content-Security-Policy-Report-Only header found. It allows for testing different directives to determine how the current policy can be trimmed or modified to create the most restrictive policy possible, however still allowing all required resources. CSP header missing on the link: GET https://archibus.vodacom.co.za/docs/realm-howto.html response code: 404

Content-Security-Policy: Header missing, but Content-Security-Policy-Report-Only header found. It allows for testing different directives to determine how the current policy can be trimmed or modified to create the most restrictive policy possible, however still allowing all required resources. CSP header missing on the link: GET https://archibus.vodacom.co.za/docs/setup.html response code: 404

Content-Security-Policy: Header missing, but Content-Security-Policy-Report-Only header found. It allows for testing different directives to determine how the current policy can be trimmed or modified to create the most restrictive policy possible, however still allowing all required resources. CSP header missing on the link: GET https://archibus.vodacom.co.za/docs/appdev/ response code: 404

Content-Security-Policy: Header missing, but Content-Security-Policy-Report-Only header found. It allows for testing different directives to determine how the current policy can be trimmed or modified to create the most restrictive policy possible, however still allowing all required resources. CSP header missing on the link: GET https://archibus.vodacom.co.za/docs/changelog.html response code: 404

Content-Security-Policy: Header missing, but Content-Security-Policy-Report-Only header found. It allows for testing different directives to determine how the current policy can be trimmed or modified to create the most restrictive policy possible, however still allowing all required resources. CSP header missing on the link: GET https://archibus.vodacom.co.za/docs/jndi-datasource-examples-howto.html response code: 404

Content-Security-Policy: Header missing, but Content-Security-Policy-Report-Only header found. It allows for testing different directives to determine how the current policy can be trimmed or modified to create the most restrictive policy possible, however still allowing all required resources. CSP header missing on the link: GET https://archibus.vodacom.co.za/docs/RELEASE-NOTES.txt response code: 404

Content-Security-Policy: Header missing, but Content-Security-Policy-Report-Only header found. It allows for testing different directives to determine how the current policy can be trimmed or modified to create the most restrictive policy possible, however still allowing all required resources. CSP header missing on the link: GET https://archibus.vodacom.co.za/_Incapsula_Resource?SWJIYLWA=719d34d31c8e3a6e6fffd425f7e032f3&ns=8&cb=1640283353 response code: 200

Content-Security-Policy: Header missing, but Content-Security-Policy-Report-Only header found. It allows for testing different directives to determine how the current policy can be trimmed or modified to create the most restrictive policy possible, however still allowing all required resources. CSP header missing on the link: GET https://archibus.vodacom.co.za/docs/deployer-howto.html response code: 404

Content-Security-Policy: Header missing, but Content-Security-Policy-Report-Only header found. It allows for testing different directives to determine how the current policy can be trimmed or modified to create the most restrictive policy possible, however still allowing all required resources. CSP header missing on the link: GET https://archibus.vodacom.co.za/docs/api/index.html response code: 404

Content-Security-Policy: Header missing, but Content-Security-Policy-Report-Only header found. It allows for testing different directives to determine how the current policy can be trimmed or modified to create the most restrictive policy possible, however still allowing all required resources. CSP header missing on the link: GET https://archibus.vodacom.co.za/FPRWin/index.aspx response code: 401

Content-Security-Policy: Header missing, but Content-Security-Policy-Report-Only header found. It allows for testing different directives to determine how the current policy can be trimmed or modified to create the most restrictive policy possible, however still allowing all required resources. CSP header missing on the link: GET https://archibus.vodacom.co.za/_Incapsula_Resource?SWJIYLWA=719d34d31c8e3a6e6fffd425f7e032f3&ns=3&cb=1880170645 response code: 200

Content-Security-Policy: Header missing, but Content-Security-Policy-Report-Only header found. It allows for testing different directives to determine how the current policy can be trimmed or modified to create the most restrictive policy possible, however still allowing all required resources. CSP header missing on the link: GET https://archibus.vodacom.co.za/Leasure-the-deed-will-the-

clipt-Angely-ands-Banq?d=archibus.vodacom.co.za response code: 200

Content-Security-Policy: Header missing, but Content-Security-Policy-Report-Only header found. It allows for testing different directives to determine how the current policy can be trimmed or modified to create the most restrictive policy possible, however still allowing all required resources. CSP header missing on the link: GET https://archibus.vodacom.co.za/_Incapsula_Resource?SWKMTFSR=1&e=0.5329770916436014 response code: 200

Content-Security-Policy: Header missing, but Content-Security-Policy-Report-Only header found. It allows for testing different directives to determine how the current policy can be trimmed or modified to create the most restrictive policy possible, however still allowing all required resources. CSP header missing on the link: GET https://archibus.vodacom.co.za/_Incapsula_Resource?SWJIYLWA=719d34d31c8e3a6e6fffd425f7e032f3&ns=21&cb=1906011217 response code: 200

Content-Security-Policy: Header missing, but Content-Security-Policy-Report-Only header found. It allows for testing different directives to determine how the current policy can be trimmed or modified to create the most restrictive policy possible, however still allowing all required resources. CSP header missing on the link: GET https://archibus.vodacom.co.za/_Incapsula_Resource?SWJIYLWA=719d34d31c8e3a6e6fffd425f7e032f3%22ns=15%22cb=422869281 response code: 200

Content-Security-Policy: Header missing, but Content-Security-Policy-Report-Only header found. It allows for testing different directives to determine how the current policy can be trimmed or modified to create the most restrictive policy possible, however still allowing all required resources. CSP header missing on the link: GET https://archibus.vodacom.co.za/_Incapsula_Resource?SWJIYLWA=719d34d31c8e3a6e6fffd425f7e032f3&ns=15&cb=422869281 response code: 200

Content-Security-Policy: Header missing, but Content-Security-Policy-Report-Only header found. It allows for testing different directives to determine how the current policy can be trimmed or modified to create the most restrictive policy possible, however still allowing all required resources. CSP header missing on the link: GET https://archibus.vodacom.co.za/_Incapsula_Resource?SWKMTFSR=1&e=0.7902679497011122 response code: 200

Content-Security-Policy: Header missing, but Content-Security-Policy-Report-Only header found. It allows for testing different directives to determine how the current policy can be trimmed or modified to create the most restrictive policy possible, however still allowing all required resources. CSP header missing on the link: GET https://archibus.vodacom.co.za/_Incapsula_Resource?SWJIYLWA=719d34d31c8e3a6e6fffd425f7e032f3&ns=30&cb=944403151 response code: 200

Content-Security-Policy: Header missing, but Content-Security-Policy-Report-Only header found. It allows for testing different directives to determine how the current policy can be trimmed or modified to create the most restrictive policy possible, however still allowing all required resources. CSP header missing on the link: GET https://archibus.vodacom.co.za/_Incapsula_Resource?SWJIYLWA=719d34d31c8e3a6e6fffd425f7e032f3%22ns=23%22cb=1610054286 response code: 200

Content-Security-Policy: Header missing, but Content-Security-Policy-Report-Only header found. It allows for testing different directives to determine how the current policy can be trimmed or modified to create the most restrictive policy possible, however still allowing all required resources. CSP header missing on the link: GET https://archibus.vodacom.co.za/_Incapsula_Resource?SWJIYLWA=719d34d31c8e3a6e6fffd425f7e032f3&ns=23&cb=1610054286 response code: 200

Content-Security-Policy: Header missing, but Content-Security-Policy-Report-Only header found. It allows for testing different directives to determine how the current policy can be trimmed or modified to create the most restrictive policy possible, however still allowing all required resources. CSP header missing on the link: GET https://archibus.vodacom.co.za/_Incapsula_Resource?SWKMTFSR=1&e=0.6767940789579447 response code: 200

Content-Security-Policy: Header missing, but Content-Security-Policy-Report-Only header found. It allows for testing different directives to determine how the current policy can be trimmed or modified to create the most restrictive policy possible, however still allowing all required resources. CSP header missing on the link: GET https://archibus.vodacom.co.za/_Incapsula_Resource?SWJIYLWA=719d34d31c8e3a6e6fffd425f7e032f3&ns=39&cb=1894920283 response code: 200

Content-Security-Policy: Header missing, but Content-Security-Policy-Report-Only header found. It allows for testing different directives to determine how the current policy can be trimmed or modified to create the most restrictive policy possible, however still allowing all required resources. CSP header missing on the link: GET https://archibus.vodacom.co.za/_Incapsula_Resource?SWJIYLWA=719d34d31c8e3a6e6fffd425f7e032f3%22ns=32%22cb=939041622 response code: 200

Content-Security-Policy: Header missing, but Content-Security-Policy-Report-Only header found. It allows for testing different directives to determine how the current policy can be trimmed or modified to create the most restrictive policy possible, however still allowing all required resources. CSP header missing on the link: GET https://archibus.vodacom.co.za/_Incapsula_Resource?SWJIYLWA=719d34d31c8e3a6e6fffd425f7e032f3&ns=32&cb=939041622 response code: 200

Content-Security-Policy: Header missing, but Content-Security-Policy-Report-Only header found. It allows for testing different directives to determine how the current policy can be trimmed or modified to create the most restrictive policy possible, however still allowing all required resources. CSP header missing on the link: GET https://archibus.vodacom.co.za/_Incapsula_Resource?SWJIYLWA=719d34d31c8e3a6e6fffd425f7e032f3%22ns=41%22cb=1973595680 response code: 200

Content-Security-Policy: Header missing, but Content-Security-Policy-Report-Only header found. It allows for testing different directives to determine how the current policy can be trimmed or modified to create the most restrictive policy possible, however still allowing all required resources. CSP header missing on the link: GET https://archibus.vodacom.co.za/_Incapsula_Resource?SWKMTFSR=1&e=0.8560383602618578 response code: 200

Content-Security-Policy: Header missing, but Content-Security-Policy-Report-Only header found. It allows for testing different directives to determine how the current policy can be trimmed or modified to create the most restrictive policy possible, however still allowing all required resources. CSP header missing on the link: GET https://archibus.vodacom.co.za/_Incapsula_Resource?SWKMTFSR=1&e=0.4472103130471645 response code: 200

Content-Security-Policy: Header missing, but Content-Security-Policy-Report-Only header found. It allows for testing different directives to determine how the current policy can be trimmed or modified to create the most restrictive policy possible, however still allowing all required resources. CSP header missing on the link: GET https://archibus.vodacom.co.za/_Incapsula_Resource?SWJIYLWA=719d34d31c8e3a6e6fffd425f7e032f3%22ns=44%22cb=974130296 response code: 200

Content-Security-Policy: Header missing, but Content-Security-Policy-Report-Only header found. It allows for testing different directives to determine how the current policy can be trimmed or modified to create the most restrictive policy possible, however still allowing all required resources. CSP header missing on the link: GET https://archibus.vodacom.co.za/_Incapsula_Resource?SWKMTFSR=1&e=0.913395824408842 response code: 200

Content-Security-Policy: Header missing, but Content-Security-Policy-Report-Only header found. It allows for testing different directives to determine how the current policy can be trimmed or modified to create the most restrictive policy possible, however still allowing all required resources. CSP header missing on the link: GET https://archibus.vodacom.co.za/_Incapsula_Resource?SWKMTFSR=1&e=0.4981508946970825 response code: 200

Content-Security-Policy: Header missing, but Content-Security-Policy-Report-Only header found. It allows for testing different directives to determine how the current policy can be trimmed or modified to create the most restrictive policy possible, however still allowing all required resources. CSP header missing on the link: GET https://archibus.vodacom.co.za/_Incapsula_Resource?SWJIYLWA=719d34d31c8e3a6e6fffd425f7e032f3%22ns=47%22cb=823359384 response code: 200

Content-Security-Policy: Header missing, but Content-Security-Policy-Report-Only header found. It allows for testing different directives to determine how the current policy can be trimmed or modified to create the most restrictive policy possible, however still allowing all required resources. CSP header missing on the link: GET https://archibus.vodacom.co.za/host-manager/ response code: 404

Content-Security-Policy: Header missing, but Content-Security-Policy-Report-Only header found. It allows for testing different directives to determine how the current policy can be trimmed or modified to create the most restrictive policy possible, however still allowing all required resources. CSP header missing on the link: GET https://archibus.vodacom.co.za/manager/ response code: 404

Content-Security-Policy: Header missing, but Content-Security-Policy-Report-Only header found. It allows for testing different directives to determine how the current policy can be trimmed or modified to create the most restrictive policy possible, however still allowing all required resources. CSP header missing on the link: GET https://archibus.vodacom.co.za/_Incapsula_Resource?SWJIYLWA=719d34d31c8e3a6e6fffd425f7e032f3%22ns=62%22cb=48444639 response code: 200

Content-Security-Policy: Header missing, but Content-Security-Policy-Report-Only header found. It allows for testing different directives to determine how the current policy can be trimmed or modified to create the most restrictive policy possible, however still allowing all required resources. CSP header missing on the link: GET https://archibus.vodacom.co.za/_Incapsula_Resource?SWKMTFSR=1&e=0.7227896506086273 response code: 200

Content-Security-Policy: Header missing, but Content-Security-Policy-Report-Only header found. It allows for testing different directives to determine how the current policy can be trimmed or modified to create the most restrictive policy possible, however still allowing all required resources. CSP header missing on the link: GET https://archibus.vodacom.co.za/_Incapsula_Resource?SWJIYLWA=719d34d31c8e3a6e6fffd425f7e032f3%22ns=64%22cb=555618287 response code: 200

Content-Security-Policy: Header missing, but Content-Security-Policy-Report-Only header found. It allows for testing different directives to determine how the current policy can be trimmed or modified to create the most restrictive policy possible, however still allowing all required resources. CSP header missing on the link: GET https://archibus.vodacom.co.za/docs/api/ response code: 404

Content-Security-Policy: Header missing, but Content-Security-Policy-Report-Only header found. It allows for testing different directives to determine how the current policy can be trimmed or modified to create the most restrictive policy possible, however still allowing all required resources. CSP header missing on the link: GET https://archibus.vodacom.co.za/FPRWin/ response code: 401

150208 Missing header: Referrer-Policy (1)

150208 Missing header: Referrer-Policy

archibus.vodacom.co.za

Finding #	10510074	**Severity**	Information Gathered - Level 2
Unique #	4409189d-1dee-430e-bd92-273f9cf4dbe8		
Group	Security Weaknesses		
CWE	CWE-16, CWE-1032	**Detection Date**	11 Feb 2024 21:02 GMT+0200
OWASP	A5 Security Misconfiguration		
WASC	WASC-15 APPLICATION MISCONFIGURATION		

Details

Threat

No Referrer Policy is specified for the link. WAS checks for the missing Referrer Policy on all static and dynamic pages. It checks for one of the following Referrer Policy in the response headers:

1) no-referrer
2) no-referrer-when-downgrade
3) same-origin
4) origin
5) origin-when-cross-origin
6) strict-origin
7) strict-origin-when-cross-origin

If the Referrer Policy header is not found , WAS checks in response body for meta tag containing tag name as "referrer" and one of the above Referrer Policy.

Impact

The Referrer-Policy header controls how much referrer information is sent to a site when navigating to it. Absence of Referrer-Policy header can lead to leakage of sensitive information via the referrer header.

Solution

Referrer Policy header improves security by ensuring websites don't leak sensitive information via the referrer header. It's recommended to add secure Referrer Policies as a part of a defense-in-depth approach.

References:
- https://www.w3.org/TR/referrer-policy/
- https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/Referrer-Policy

Results

Referrer-Policy: Header missing
Response headers on link: GET https://archibus.vodacom.co.za/Leasure-the-deed-will-the-clipt-Angely-ands-Banq response code: 200

Cache-Control: max-age=47, public
Content-Encoding: gzip
Content-Length: 77738
Content-Security-Policy-Report-Only: default-src 'self' 'unsafe-eval' 'unsafe-hashes' 'unsafe-inline' data: blob: ; form-action 'none' data: blob: ; report-uri /csp_report
Content-Type: text/javascript
Date: Sun, 11 Feb 2024 19:03:30 GMT
Etag: "4df2a20d"
Expires: Sun, 11 Feb 2024 19:04:17 GMT
X-CDN: Imperva
X-Iinfo: 56-11943627-0 0CNN RT(1707678199943 10992) q(0 -1 -1 -1) r(0 -1)
Set-Cookie: visid_incap_2776849=FzwYQrB5SDmrEoE8GapjSPYZyWUAAAAAQUIPAAAAAACKSeVsUKW+PDQEFi62u5/P; HttpOnly; expires=Sun, 09-Feb-2025 22:21:11 GMT; domain=.vodacom.co.za; path=/
Set-Cookie: nlbi_2776849=2+b7ZdTvP3ssIFAPZU49BAAAAAATg/RB/1C/i+jo3xrjvYzk; domain=.vodacom.co.za; path=/
Set-Cookie: incap_ses_1687_2776849=lxYnX5C6qRDb7PgfvG1pF/YZyWUAAAAAg7Eia1/rhUGqMH+aaFiXQA==; domain=.vodacom.co.za; path=/
Set-Cookie: nlbi_2776849_2147483392=WoCbbZ/T0xODuuO8ZU49BAAAAAC4rTMSqcwSp5j8m2+NYJTV; domain=.vodacom.co.za; path=/

Header missing on the following link(s):
(Only first 50 such pages are listed)

GET https://archibus.vodacom.co.za/Leasure-the-deed-will-the-clipt-Angely-ands-Banq response code: 200
GET https://archibus.vodacom.co.za/favicon.ico response code: 200
GET https://archibus.vodacom.co.za/tomcat.css response code: 200
GET https://archibus.vodacom.co.za/docs/ response code: 404
GET https://archibus.vodacom.co.za/docs/config/ response code: 404
GET https://archibus.vodacom.co.za/examples/ response code: 404
GET https://archibus.vodacom.co.za/docs/cluster-howto.html response code: 404
GET https://archibus.vodacom.co.za/docs/security-howto.html response code: 404
GET https://archibus.vodacom.co.za/docs/manager-howto.html response code: 404
GET https://archibus.vodacom.co.za/manager/status response code: 404
GET https://archibus.vodacom.co.za/manager/html response code: 404
GET https://archibus.vodacom.co.za/host-manager/html response code: 404
GET https://archibus.vodacom.co.za/docs/realm-howto.html response code: 404
GET https://archibus.vodacom.co.za/docs/setup.html response code: 404
GET https://archibus.vodacom.co.za/docs/appdev/ response code: 404
GET https://archibus.vodacom.co.za/docs/changelog.html response code: 404
GET https://archibus.vodacom.co.za/docs/jndi-datasource-examples-howto.html response code: 404
GET https://archibus.vodacom.co.za/docs/RELEASE-NOTES.txt response code: 404
GET https://archibus.vodacom.co.za/_Incapsula_Resource?SWJIYLWA=719d34d31c8e3a6e6fffd425f7e032f3&ns=8&cb=1640283353 response code: 200
GET https://archibus.vodacom.co.za/docs/deployer-howto.html response code: 404
GET https://archibus.vodacom.co.za/docs/api/index.html response code: 404
GET https://archibus.vodacom.co.za/FPRWin/index.aspx response code: 401
GET https://archibus.vodacom.co.za/_Incapsula_Resource?SWJIYLWA=719d34d31c8e3a6e6fffd425f7e032f3&ns=3&cb=1880170645 response code: 200
GET https://archibus.vodacom.co.za/Leasure-the-deed-will-the-clipt-Angely-ands-Banq?d=archibus.vodacom.co.za response code: 200
GET https://archibus.vodacom.co.za/_Incapsula_Resource?SWKMTFSR=1&e=0.5329770916436014 response code: 200
GET https://archibus.vodacom.co.za/_Incapsula_Resource?SWJIYLWA=719d34d31c8e3a6e6fffd425f7e032f3&ns=21&cb=1906011217 response code: 200
GET https://archibus.vodacom.co.za/_Incapsula_Resource?SWJIYLWA=719d34d31c8e3a6e6fffd425f7e032f3%22ns=15%22cb=422869281 response code: 200
GET https://archibus.vodacom.co.za/_Incapsula_Resource?SWJIYLWA=719d34d31c8e3a6e6fffd425f7e032f3&ns=15&cb=422869281 response code: 200
GET https://archibus.vodacom.co.za/_Incapsula_Resource?SWKMTFSR=1&e=0.7902679497011122 response code: 200
GET https://archibus.vodacom.co.za/_Incapsula_Resource?SWJIYLWA=719d34d31c8e3a6e6fffd425f7e032f3&ns=30&cb=944403151 response code: 200
GET https://archibus.vodacom.co.za/_Incapsula_Resource?SWJIYLWA=719d34d31c8e3a6e6fffd425f7e032f3%22ns=23%22cb=1610054286 response code: 200
GET https://archibus.vodacom.co.za/_Incapsula_Resource?SWJIYLWA=719d34d31c8e3a6e6fffd425f7e032f3&ns=23&cb=1610054286 response code: 200
GET https://archibus.vodacom.co.za/_Incapsula_Resource?SWKMTFSR=1&e=0.6767940789579447 response code: 200
GET https://archibus.vodacom.co.za/_Incapsula_Resource?SWJIYLWA=719d34d31c8e3a6e6fffd425f7e032f3&ns=39&cb=1894920283 response code: 200
GET https://archibus.vodacom.co.za/_Incapsula_Resource?SWJIYLWA=719d34d31c8e3a6e6fffd425f7e032f3%22ns=32%22cb=939041622 response code: 200
GET https://archibus.vodacom.co.za/_Incapsula_Resource?SWJIYLWA=719d34d31c8e3a6e6fffd425f7e032f3&ns=32&cb=939041622 response code: 200
GET https://archibus.vodacom.co.za/_Incapsula_Resource?SWJIYLWA=719d34d31c8e3a6e6fffd425f7e032f3%22ns=41%22cb=1973595680 response code: 200
GET https://archibus.vodacom.co.za/_Incapsula_Resource?SWKMTFSR=1&e=0.8560383602618578 response code: 200
GET https://archibus.vodacom.co.za/_Incapsula_Resource?SWKMTFSR=1&e=0.4472103130471645 response code: 200
GET https://archibus.vodacom.co.za/_Incapsula_Resource?SWJIYLWA=719d34d31c8e3a6e6fffd425f7e032f3%22ns=44%22cb=974130296 response code: 200
GET https://archibus.vodacom.co.za/_Incapsula_Resource?SWKMTFSR=1&e=0.913395824408842 response code: 200
GET https://archibus.vodacom.co.za/_Incapsula_Resource?SWKMTFSR=1&e=0.4981508946970825 response code: 200
GET https://archibus.vodacom.co.za/_Incapsula_Resource?SWJIYLWA=719d34d31c8e3a6e6fffd425f7e032f3%22ns=47%22cb=823359384 response code: 200
GET https://archibus.vodacom.co.za/host-manager/ response code: 404
GET https://archibus.vodacom.co.za/manager/ response code: 404
GET https://archibus.vodacom.co.za/_Incapsula_Resource?SWJIYLWA=719d34d31c8e3a6e6fffd425f7e032f3%22ns=62%22cb=48444639 response code: 200
GET https://archibus.vodacom.co.za/_Incapsula_Resource?SWKMTFSR=1&e=0.7227896506086273 response code: 200
GET https://archibus.vodacom.co.za/_Incapsula_Resource?SWJIYLWA=719d34d31c8e3a6e6fffd425f7e032f3%22ns=64%22cb=555618287 response code: 200
GET https://archibus.vodacom.co.za/docs/api/ response code: 404
GET https://archibus.vodacom.co.za/FPRWin/ response code: 401

150248 Missing header: Permissions-Policy (1)

150248 Missing header: Permissions-Policy *archibus.vodacom.co.za*

Finding #	10510082	**Severity**	Information Gathered - Level 2
Unique #	a56db2bd-a7d4-4f12-bc3d-2b529a596b4f		
Group	Security Weaknesses		
CWE	CWE-284	**Detection Date**	11 Feb 2024 21:02 GMT+0200
OWASP	A5 Security Misconfiguration		

WAS Web Application Report

WASC -

Details

Threat
The Permissions-Policy response header is not present.

Impact
Permissions-Policy allows web developers to selectively enable, disable, or modify the behavior of some of the browser features and APIs within their application.

A user agent has a set of supported features(Policy Controlled Features), which is the set of features which it allows to be controlled through policies.

Not defining policy for unused and risky policy controlled features may leave application vulnerable.

Solution
It is recommended to define policy for policy controlled features to make application more secure.

References:
Permissions-Policy W3C Working Draft
Policy Controlled Features

Results

Permissions-Policy: Header missing
Response headers on link: GET https://archibus.vodacom.co.za/Leasure-the-deed-will-the-clipt-Angely-ands-Banq response code: 200
Cache-Control: max-age=47, public
Content-Encoding: gzip
Content-Length: 77738
Content-Security-Policy-Report-Only: default-src 'self' 'unsafe-eval' 'unsafe-hashes' 'unsafe-inline' data: blob: ; form-action 'none' data: blob: ; report-uri /csp_report
Content-Type: text/javascript
Date: Sun, 11 Feb 2024 19:03:30 GMT
Etag: "4df2a20d"
Expires: Sun, 11 Feb 2024 19:04:17 GMT
X-CDN: Imperva
X-Iinfo: 56-11943627-0 0CNN RT(1707678199943 10992) q(0 -1 -1 -1) r(0 -1)
Set-Cookie: visid_incap_2776849=FzwYQrB5SDmrEoE8GapjSPYZyWUAAAAAQUIPAAAAAACKSeVsUKW+PDQEFi62u5/P; HttpOnly; expires=Sun, 09-Feb-2025 22:21:11 GMT; domain=.vodacom.co.za; path=/
Set-Cookie: nlbi_2776849=2+b7ZdTvP3ssIFAPZU49BAAAAAATg/RB/1C/i+jo3xrjvYzk; domain=.vodacom.co.za; path=/
Set-Cookie: incap_ses_1687_2776849=lxYnX5C6qRDb7PgfvG1pF/YZyWUAAAAAg7Eia1/rhUGqMH+aaFiXQA==; domain=.vodacom.co.za; path=/
Set-Cookie: nlbi_2776849_2147483392=WoCbbZ/T0xODuuO8ZU49BAAAAAC4rTMSqcwSp5j8m2+NYJTV; domain=.vodacom.co.za; path=/

Header missing on the following link(s):
(Only first 50 such pages are listed)

GET https://archibus.vodacom.co.za/Leasure-the-deed-will-the-clipt-Angely-ands-Banq response code: 200
GET https://archibus.vodacom.co.za/favicon.ico response code: 200
GET https://archibus.vodacom.co.za/tomcat.css response code: 200
GET https://archibus.vodacom.co.za/docs/ response code: 404
GET https://archibus.vodacom.co.za/docs/config/ response code: 404
GET https://archibus.vodacom.co.za/examples/ response code: 404
GET https://archibus.vodacom.co.za/docs/cluster-howto.html response code: 404
GET https://archibus.vodacom.co.za/docs/security-howto.html response code: 404
GET https://archibus.vodacom.co.za/docs/manager-howto.html response code: 404
GET https://archibus.vodacom.co.za/manager/status response code: 404
GET https://archibus.vodacom.co.za/manager/html response code: 404
GET https://archibus.vodacom.co.za/host-manager/html response code: 404
GET https://archibus.vodacom.co.za/docs/realm-howto.html response code: 404
GET https://archibus.vodacom.co.za/docs/setup.html response code: 404
GET https://archibus.vodacom.co.za/docs/appdev/ response code: 404
GET https://archibus.vodacom.co.za/docs/changelog.html response code: 404
GET https://archibus.vodacom.co.za/docs/jndi-datasource-examples-howto.html response code: 404
GET https://archibus.vodacom.co.za/docs/RELEASE-NOTES.txt response code: 404
GET https://archibus.vodacom.co.za/_Incapsula_Resource?SWJIYLWA=719d34d31c8e3a6e6fffd425f7e032f3&ns=8&cb=1640283353 response code: 200
GET https://archibus.vodacom.co.za/docs/deployer-howto.html response code: 404
GET https://archibus.vodacom.co.za/docs/api/index.html response code: 404
GET https://archibus.vodacom.co.za/FPRWin/index.aspx response code: 401
GET https://archibus.vodacom.co.za/_Incapsula_Resource?SWJIYLWA=719d34d31c8e3a6e6fffd425f7e032f3&ns=3&cb=1880170645 response code: 200

GET https://archibus.vodacom.co.za/Leasure-the-deed-will-the-clipt-Angely-ands-Banq?d=archibus.vodacom.co.za response code: 200
GET https://archibus.vodacom.co.za/_Incapsula_Resource?SWKMTFSR=1&e=0.5329770916436014 response code: 200
GET https://archibus.vodacom.co.za/_Incapsula_Resource?SWJIYLWA=719d34d31c8e3a6e6fffd425f7e032f3&ns=21&cb=1906011217 response code: 200
GET https://archibus.vodacom.co.za/_Incapsula_Resource?SWJIYLWA=719d34d31c8e3a6e6fffd425f7e032f3%22ns=15%22cb=422869281 response code: 200
GET https://archibus.vodacom.co.za/_Incapsula_Resource?SWJIYLWA=719d34d31c8e3a6e6fffd425f7e032f3&ns=15&cb=422869281 response code: 200
GET https://archibus.vodacom.co.za/_Incapsula_Resource?SWKMTFSR=1&e=0.7902679497011122 response code: 200
GET https://archibus.vodacom.co.za/_Incapsula_Resource?SWJIYLWA=719d34d31c8e3a6e6fffd425f7e032f3&ns=30&cb=944403151 response code: 200
GET https://archibus.vodacom.co.za/_Incapsula_Resource?SWJIYLWA=719d34d31c8e3a6e6fffd425f7e032f3%22ns=23%22cb=1610054286 response code: 200
GET https://archibus.vodacom.co.za/_Incapsula_Resource?SWJIYLWA=719d34d31c8e3a6e6fffd425f7e032f3&ns=23&cb=1610054286 response code: 200
GET https://archibus.vodacom.co.za/_Incapsula_Resource?SWKMTFSR=1&e=0.6767940789579447 response code: 200
GET https://archibus.vodacom.co.za/_Incapsula_Resource?SWJIYLWA=719d34d31c8e3a6e6fffd425f7e032f3&ns=39&cb=1894920283 response code: 200
GET https://archibus.vodacom.co.za/_Incapsula_Resource?SWJIYLWA=719d34d31c8e3a6e6fffd425f7e032f3%22ns=32%22cb=939041622 response code: 200
GET https://archibus.vodacom.co.za/_Incapsula_Resource?SWJIYLWA=719d34d31c8e3a6e6fffd425f7e032f3&ns=32&cb=939041622 response code: 200
GET https://archibus.vodacom.co.za/_Incapsula_Resource?SWJIYLWA=719d34d31c8e3a6e6fffd425f7e032f3%22ns=41%22cb=1973595680 response code: 200
GET https://archibus.vodacom.co.za/_Incapsula_Resource?SWKMTFSR=1&e=0.8560383602618578 response code: 200
GET https://archibus.vodacom.co.za/_Incapsula_Resource?SWKMTFSR=1&e=0.4472103130471645 response code: 200
GET https://archibus.vodacom.co.za/_Incapsula_Resource?SWJIYLWA=719d34d31c8e3a6e6fffd425f7e032f3%22ns=44%22cb=974130296 response code: 200
GET https://archibus.vodacom.co.za/_Incapsula_Resource?SWKMTFSR=1&e=0.913395824408842 response code: 200
GET https://archibus.vodacom.co.za/_Incapsula_Resource?SWKMTFSR=1&e=0.4981508946970825 response code: 200
GET https://archibus.vodacom.co.za/_Incapsula_Resource?SWJIYLWA=719d34d31c8e3a6e6fffd425f7e032f3%22ns=47%22cb=823359384 response code: 200
GET https://archibus.vodacom.co.za/host-manager/ response code: 404
GET https://archibus.vodacom.co.za/manager/ response code: 404
GET https://archibus.vodacom.co.za/_Incapsula_Resource?SWJIYLWA=719d34d31c8e3a6e6fffd425f7e032f3%22ns=62%22cb=48444639 response code: 200
GET https://archibus.vodacom.co.za/_Incapsula_Resource?SWKMTFSR=1&e=0.7227896506086273 response code: 200
GET https://archibus.vodacom.co.za/_Incapsula_Resource?SWJIYLWA=719d34d31c8e3a6e6fffd425f7e032f3%22ns=64%22cb=555618287 response code: 200
GET https://archibus.vodacom.co.za/docs/api/ response code: 404
GET https://archibus.vodacom.co.za/FPRWin/ response code: 401

150249 Misconfigured Header: Cache-Control (1)

150249 Misconfigured Header: Cache-Control

archibus.vodacom.co.za

Finding #	10974668	**Severity**	Information Gathered - Level 2
Unique #	8be36be0-964d-4b42-815c-b7b8f538a47d		
Group	Security Weaknesses		
CWE	CWE-525	**Detection Date**	11 Feb 2024 21:02 GMT+0200
OWASP	A5 Security Misconfiguration		
WASC	-		

Details

Threat

Cache-Control header present but directives may not configured to adequately safeguard sensitive information.

For Example:
Cache-Control directive set to public.

max-age value is greater than 86400.

Impact

If directive is set to public, the resource can be stored by any cache.

If max-age value is greater than 86400 for sensitive information may lead to information leakage.

Solution

Please check that resources with sensitive information are not configured with Cache-Control public directive.

Also please make sure that max-age directive value set properly to not cache sensitive information for longer period than needed.

References:
Mozilla Documentation Cache-Control

WAS Web Application Report

Results

Cache-Control: Header misconfigured. Cache-Control public directive found.
Cache-Control:max-age=47, public on the link: GET https://archibus.vodacom.co.za/Leasure-the-deed-will-the-clipt-Angely-ands-Banq response code: 200

Cache-Control: Header misconfigured. Cache-Control public directive found.
Cache-Control:max-age=86383, public on the link: GET https://archibus.vodacom.co.za/favicon.ico response code: 200

Cache-Control: Header misconfigured. Cache-Control public directive found.
Cache-Control:max-age=4, public on the link: GET https://archibus.vodacom.co.za/Leasure-the-deed-will-the-clipt-Angely-ands-Banq?d=archibus.vodacom.co.za response code: 200

150262 Missing header: Feature-Policy (1)

150262 Missing header: Feature-Policy

archibus.vodacom.co.za

Finding #	10510087	**Severity**	Information Gathered - Level 2
Unique #	c3bf3e00-f76b-4b5a-aac7-f2fa44b51900		
Group	Security Weaknesses		
CWE	CWE-16, CWE-1032	**Detection Date**	11 Feb 2024 21:02 GMT+0200
OWASP	A5 Security Misconfiguration		
WASC	WASC-15 APPLICATION MISCONFIGURATION		

Details

Threat

The Feature-Policy response header is not present.

Impact

Feature Policy allows web developers to selectively enable, disable, and modify the behavior of certain APIs and web features such as "geolocation","camera", "usb", "fullscreen", "animations" etc in the browser.

These policies restrict what APIs the site can access or modify the browser's default behavior for certain features.

Solution

It is recommended to set the Feature-Policy header to selectively enable, disable, and modify the behavior of certain APIs and web features.

References:
- https://www.w3.org/TR/feature-policy/
- https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/Feature-Policy

Results

Feature-Policy: Header missing
Response headers on link: GET https://archibus.vodacom.co.za/Leasure-the-deed-will-the-clipt-Angely-ands-Banq response code: 200
Cache-Control: max-age=47, public
Content-Encoding: gzip
Content-Length: 77738
Content-Security-Policy-Report-Only: default-src 'self' 'unsafe-eval' 'unsafe-hashes' 'unsafe-inline' data: blob: ; form-action 'none' data: blob: ; report-uri /csp_report
Content-Type: text/javascript
Date: Sun, 11 Feb 2024 19:03:30 GMT
Etag: "4df2a20d"
Expires: Sun, 11 Feb 2024 19:04:17 GMT
X-CDN: Imperva
X-Iinfo: 56-11943627-0 0CNN RT(1707678199943 10992) q(0 -1 -1 -1) r(0 -1)
Set-Cookie: visid_incap_2776849=FzwYQrB5SDmrEoE8GapjSPYZyWUAAAAAQUIPAAAAAACKSeVsUKW+PDQEFi62u5/P; HttpOnly; expires=Sun, 09-Feb-2025 22:21:11 GMT; domain=.vodacom.co.za; path=/
Set-Cookie: nlbi_2776849=2+b7ZdTvP3ssIFAPZU49BAAAAAATg/RB/1C/i+jo3xrjvYzk; domain=.vodacom.co.za; path=/
Set-Cookie: incap_ses_1687_2776849=lxYnX5C6qRDb7PgfvG1pF/YZyWUAAAAAg7Eia1/rhUGqMH+aaFiXQA==; domain=.vodacom.co.za; path=/
Set-Cookie: nlbi_2776849_2147483392=WoCbbZ/T0xODuuO8ZU49BAAAAAC4rTMSqcwSp5j8m2+NYJTV; domain=.vodacom.co.za; path=/

Header missing on the following link(s):
(Only first 50 such pages are listed)

GET https://archibus.vodacom.co.za/Leasure-the-deed-will-the-clipt-Angely-ands-Banq response code: 200
GET https://archibus.vodacom.co.za/favicon.ico response code: 200
GET https://archibus.vodacom.co.za/tomcat.css response code: 200
GET https://archibus.vodacom.co.za/docs/ response code: 404
GET https://archibus.vodacom.co.za/docs/config/ response code: 404
GET https://archibus.vodacom.co.za/examples/ response code: 404
GET https://archibus.vodacom.co.za/docs/cluster-howto.html response code: 404
GET https://archibus.vodacom.co.za/docs/security-howto.html response code: 404
GET https://archibus.vodacom.co.za/docs/manager-howto.html response code: 404
GET https://archibus.vodacom.co.za/manager/status response code: 404
GET https://archibus.vodacom.co.za/manager/html response code: 404
GET https://archibus.vodacom.co.za/host-manager/html response code: 404
GET https://archibus.vodacom.co.za/docs/realm-howto.html response code: 404
GET https://archibus.vodacom.co.za/docs/setup.html response code: 404
GET https://archibus.vodacom.co.za/docs/appdev/ response code: 404
GET https://archibus.vodacom.co.za/docs/changelog.html response code: 404
GET https://archibus.vodacom.co.za/docs/jndi-datasource-examples-howto.html response code: 404
GET https://archibus.vodacom.co.za/docs/RELEASE-NOTES.txt response code: 404
GET https://archibus.vodacom.co.za/_Incapsula_Resource?SWJIYLWA=719d34d31c8e3a6e6fffd425f7e032f3&ns=8&cb=1640283353 response code: 200
GET https://archibus.vodacom.co.za/docs/deployer-howto.html response code: 404
GET https://archibus.vodacom.co.za/docs/api/index.html response code: 404
GET https://archibus.vodacom.co.za/FPRWin/index.aspx response code: 401
GET https://archibus.vodacom.co.za/_Incapsula_Resource?SWJIYLWA=719d34d31c8e3a6e6fffd425f7e032f3&ns=3&cb=1880170645 response code: 200
GET https://archibus.vodacom.co.za/Leasure-the-deed-will-the-clipt-Angely-ands-Banq?d=archibus.vodacom.co.za response code: 200
GET https://archibus.vodacom.co.za/_Incapsula_Resource?SWKMTFSR=1&e=0.5329770916436014 response code: 200
GET https://archibus.vodacom.co.za/_Incapsula_Resource?SWJIYLWA=719d34d31c8e3a6e6fffd425f7e032f3&ns=21&cb=1906011217 response code: 200
GET https://archibus.vodacom.co.za/_Incapsula_Resource?SWJIYLWA=719d34d31c8e3a6e6fffd425f7e032f3%22ns=15%22cb=422869281 response code: 200
GET https://archibus.vodacom.co.za/_Incapsula_Resource?SWJIYLWA=719d34d31c8e3a6e6fffd425f7e032f3&ns=15&cb=422869281 response code: 200
GET https://archibus.vodacom.co.za/_Incapsula_Resource?SWKMTFSR=1&e=0.7902679497011122 response code: 200
GET https://archibus.vodacom.co.za/_Incapsula_Resource?SWJIYLWA=719d34d31c8e3a6e6fffd425f7e032f3&ns=30&cb=944403151 response code: 200
GET https://archibus.vodacom.co.za/_Incapsula_Resource?SWJIYLWA=719d34d31c8e3a6e6fffd425f7e032f3%22ns=23%22cb=1610054286 response code: 200
GET https://archibus.vodacom.co.za/_Incapsula_Resource?SWJIYLWA=719d34d31c8e3a6e6fffd425f7e032f3&ns=23&cb=1610054286 response code: 200
GET https://archibus.vodacom.co.za/_Incapsula_Resource?SWKMTFSR=1&e=0.6767940789579447 response code: 200
GET https://archibus.vodacom.co.za/_Incapsula_Resource?SWJIYLWA=719d34d31c8e3a6e6fffd425f7e032f3&ns=39&cb=1894920283 response code: 200
GET https://archibus.vodacom.co.za/_Incapsula_Resource?SWJIYLWA=719d34d31c8e3a6e6fffd425f7e032f3%22ns=32%22cb=939041622 response code: 200
GET https://archibus.vodacom.co.za/_Incapsula_Resource?SWJIYLWA=719d34d31c8e3a6e6fffd425f7e032f3&ns=32&cb=939041622 response code: 200
GET https://archibus.vodacom.co.za/_Incapsula_Resource?SWJIYLWA=719d34d31c8e3a6e6fffd425f7e032f3%22ns=41%22cb=1973595680 response code: 200
GET https://archibus.vodacom.co.za/_Incapsula_Resource?SWKMTFSR=1&e=0.8560383602618578 response code: 200
GET https://archibus.vodacom.co.za/_Incapsula_Resource?SWKMTFSR=1&e=0.4472103130471645 response code: 200
GET https://archibus.vodacom.co.za/_Incapsula_Resource?SWJIYLWA=719d34d31c8e3a6e6fffd425f7e032f3%22ns=44%22cb=974130296 response code: 200
GET https://archibus.vodacom.co.za/_Incapsula_Resource?SWKMTFSR=1&e=0.913395824408842 response code: 200
GET https://archibus.vodacom.co.za/_Incapsula_Resource?SWKMTFSR=1&e=0.4981508946970825 response code: 200
GET https://archibus.vodacom.co.za/_Incapsula_Resource?SWJIYLWA=719d34d31c8e3a6e6fffd425f7e032f3%22ns=47%22cb=823359384 response code: 200
GET https://archibus.vodacom.co.za/host-manager/ response code: 404
GET https://archibus.vodacom.co.za/manager/ response code: 404
GET https://archibus.vodacom.co.za/_Incapsula_Resource?SWJIYLWA=719d34d31c8e3a6e6fffd425f7e032f3%22ns=62%22cb=48444639 response code: 200
GET https://archibus.vodacom.co.za/_Incapsula_Resource?SWKMTFSR=1&e=0.7227896506086273 response code: 200
GET https://archibus.vodacom.co.za/_Incapsula_Resource?SWJIYLWA=719d34d31c8e3a6e6fffd425f7e032f3%22ns=64%22cb=555618287 response code: 200
GET https://archibus.vodacom.co.za/docs/api/ response code: 404
GET https://archibus.vodacom.co.za/FPRWin/ response code: 401

150126 Links With High Resource Consumption (1)

150126 Links With High Resource Consumption

archibus.vodacom.co.za

Finding #	14173447	**Severity**	Information Gathered - Level 1
Unique #	f4597af9-ed34-4b4e-aef1-7e3cbf089655		
Group	Security Weaknesses		
CWE	-	**Detection Date**	11 Feb 2024 21:02 GMT+0200
OWASP	-		
WASC	-		

Details

Threat

The list of links with lowest bytes/sec which are assumed to be resources with highest resource consumption. The links in the list have slower transfer times speeds to an average resource on the server. This may indicate that the links are more CPU or DB intensive than majority of links.

The latency of the network and file size have no effect on calculations.

Impact
The links with high resource consumption could be used to perform DOS on the server by just performing GET Flooding. Attackers could more easily take the server down if there are huge resource hogs on it, performing less request.

Solution
Find the root cause of resources slow download speed.

If the cause is a real CPU strain or complex DB queries performed, there may be a need for re-engineering of the web application or defense measures should be in place. Examples of defense against DOS that is targeted towards high resource consumption links are Load Balancers and Rate Limiters.

Results

0.000000 bytes/sec https://archibus.vodacom.co.za/_Incapsula_Resource?SWJIYLWA=719d34d31c8e3a6e6fffd425f7e032f3%22ns=23%22cb=1610054286
0.000000 bytes/sec https://archibus.vodacom.co.za/_Incapsula_Resource?SWJIYLWA=719d34d31c8e3a6e6fffd425f7e032f3%22ns=32%22cb=939041622
0.000000 bytes/sec https://archibus.vodacom.co.za/_Incapsula_Resource?SWJIYLWA=719d34d31c8e3a6e6fffd425f7e032f3%22ns=44%22cb=974130296
0.000000 bytes/sec https://archibus.vodacom.co.za/_Incapsula_Resource?SWJIYLWA=719d34d31c8e3a6e6fffd425f7e032f3%22ns=47%22cb=823359384
0.000000 bytes/sec https://archibus.vodacom.co.za/_Incapsula_Resource?SWJIYLWA=719d34d31c8e3a6e6fffd425f7e032f3%22ns=63%22cb=837791161
0.000000 bytes/sec https://archibus.vodacom.co.za/_Incapsula_Resource?SWJIYLWA=719d34d31c8e3a6e6fffd425f7e032f3%22ns=64%22cb=555618287
0.000000 bytes/sec https://archibus.vodacom.co.za/_Incapsula_Resource?SWJIYLWA=719d34d31c8e3a6e6fffd425f7e032f3%22ns=88%22cb=1271059637
0.000000 bytes/sec https://archibus.vodacom.co.za/_Incapsula_Resource?SWJIYLWA=719d34d31c8e3a6e6fffd425f7e032f3%22ns=89%22cb=463486056
0.000000 bytes/sec https://archibus.vodacom.co.za/_Incapsula_Resource?SWJIYLWA=719d34d31c8e3a6e6fffd425f7e032f3%22ns=90%22cb=212317304
0.000000 bytes/sec https://archibus.vodacom.co.za/csp_report

150135 HTTP Strict Transport Security (HSTS) header missing or misconfigured (1)

150135 HTTP Strict Transport Security (HSTS) header missing or misconfigured — *archibus.vodacom.co.za*

Finding #	10510088	**Severity**	Information Gathered - Level 1
Unique #	bf7ee9c5-9209-451f-8f09-62b40fdae1ae		
Group	Security Weaknesses		
CWE	CWE-523	**Detection Date**	11 Feb 2024 21:02 GMT+0200
OWASP	A5 Security Misconfiguration		
WASC	-		

Details

Threat
HTTP Strict Transport Security (HSTS) header was found to be missing or misconfigured. The HSTS header instructs browsers that all subsequent connections to the website, for a configurable amount of time, should be performed over a secure (HTTPS) connection only. Additionally, it instructs browsers that users should not be permitted to bypass SSL/TLS certificate errors, in the event of an expired or otherwise untrusted certificate for example.

Impact
If HSTS header is not set, users are potentially vulnerable to man-in-the-middle (MITM) attacks, SSL stripping, and passive eavesdropper attacks.

Solution
For information about how to implement the HSTS header properly, refer to the OWASP HTTP Strict Transport Security Cheat Sheet.

Results

Strict Transport Security header missing for
https://archibus.vodacom.co.za/_Incapsula_Resource?SWKMTFSR=1&e=0.4472103130471645

150142 Virtual Host Discovered (1)

150142 Virtual Host Discovered — *archibus.vodacom.co.za*

Finding #	14173448	**Severity**	Information Gathered - Level 1

Unique #	eeb33cbe-8b83-44c5-9c88-59ceb19d6422		
Group	Security Weaknesses		
CWE	CWE-200	**Detection Date**	11 Feb 2024 21:02 GMT+0200
OWASP	A5 Security Misconfiguration		
WASC	-		

Details

Threat

Web server is responding differently when the HOST header is manipulated and various common virtual hosts are tested. This could indicate the presence of Virtual Host. Virtual hosting is a method for hosting multiple domain names (with separate handling of each name) on a single server (or pool of servers). This allows one server to share its resources, such as memory and processor cycles, without requiring all services provided to use the same host name. The extra virtual hosts discovered by the Web application scanner during HOST header manipulation are provided in the Results section.

Impact

The Web application should apply consistent security measures. If the Web application fails to apply security controls to other domains hosted on the same server, then it may be exposed to vulnerabilities like cross-site scripting, SQL injection, or authorization-based attacks.

Solution

Consult the virtual host configuration and check if this virtual host should be publicly accessible.

Results

Virtual host discovered:

Detected based on: HTTP Response code
Virtual Host: web.vodacom.co.za
URI: https://archibus.vodacom.co.za/

150204 Missing header: X-XSS-Protection (1)

150204 Missing header: X-XSS-Protection

archibus.vodacom.co.za

Finding #	10510096	**Severity**	Information Gathered - Level 1
Unique #	ec44c2bf-c94d-43e2-a6ec-d79de0e38d3b		
Group	Security Weaknesses		
CWE	CWE-16, CWE-1032	**Detection Date**	11 Feb 2024 21:02 GMT+0200
OWASP	A5 Security Misconfiguration		
WASC	WASC-15 APPLICATION MISCONFIGURATION		

Details

Threat

The X-XSS-Protection response header is not present.

Impact

The X-XSS-Protection response header provides a layer of protection against reflected cross-site scripting (XSS) attacks by instructing browsers to abort rendering a page in which a reflected XSS attack has been detected. This is a best-effort second line of defense measure which helps prevent an attacker from using evasion techniques to avoid the neutralization mechanisms that the filters use by default. When configured appropriately, browser-level XSS filters can provide additional layers of defense against web application attacks.

Note that HTTP 4xx and 5xx responses can also be susceptible to attacks such as XSS. For better security the X-XSS-Protection header should be set on 4xx and 5xx responses as well.

Solution

It is recommend to set X-XSS-Protection header with value set to '1; mode=block' on all the relevant responses to activate browser's XSS filter.

NOTE: The X-XSS-Protection header is not supported by all browsers. Google Chrome and Safari are some of the browsers which support it, Firefox on the other hand does not support the header. X-XSS-Protection header does not guarantee a complete protection against XSS. For better protection against XSS attacks, the web application should use secure coding principles. Also, consider leveraging the Content-Security-Policy (CSP) header, which is supported by all browsers.

Using X-XSS-Protection could have unintended side effects, please understand the implications carefully before using it.

References:
- https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/X-XSS-Protection
- https://blog.innerht.ml/the-misunderstood-x-xss-protection/
- https://www.mbsd.jp/blog/20160407.html
- https://www.chromium.org/developers/design-documents/xss-auditor

Results

X-Xss-Protection: Header missing
Response headers on link: GET https://archibus.vodacom.co.za/docs/ response code: 404
Connection: keep-alive
Content-Encoding: gzip
Content-Language: en
Content-Security-Policy-Report-Only: default-src 'self' 'unsafe-eval' 'unsafe-hashes' 'unsafe-inline' data: blob: ; form-action 'none' data: blob: ; report-uri /csp_report
Content-Type: text/html;charset=utf-8
Date: Sun, 11 Feb 2024 19:03:47 GMT
Instance: /ITG/pool_archibus_8082 10.134.15.35 8082
Keep-Alive: timeout=20
Transfer-Encoding: chunked
X-CDN: Imperva
X-Iinfo: 56-11943627-11943785 SNYy RT(1707678199943 26590) q(0 0 0 -1) r(2 2) U11
Set-Cookie: visid_incap_2776849=FzwYQrB5SDmrEoE8GapjSPYZyWUAAAAAQUIPAAAAAACKSeVsUKW+PDQEFi62u5/P; HttpOnly; expires=Sun, 09-Feb-2025 22:21:11 GMT; domain=.vodacom.co.za; path=/
Set-Cookie: nlbi_2776849=2+b7ZdTvP3ssIFAPZU49BAAAAAATg/RB/1C/i+jo3xrjvYzk; domain=.vodacom.co.za; path=/
Set-Cookie: incap_ses_1687_2776849=lxYnX5C6qRDb7PgfvG1pF/YZyWUAAAAAg7Eia1/rhUGqMH+aaFiXQA==; domain=.vodacom.co.za; path=/
Set-Cookie: nlbi_2776849_2147483392=+w2NJ/I5ExcKzAeXZU49BAAAAADfaPWTCAiQwC6yx6SR6MH/; domain=.vodacom.co.za; path=/

Header missing on the following link(s):
(Only first 50 such pages are listed)

GET https://archibus.vodacom.co.za/docs/ response code: 404
GET https://archibus.vodacom.co.za/docs/config/ response code: 404
GET https://archibus.vodacom.co.za/examples/ response code: 404
GET https://archibus.vodacom.co.za/docs/cluster-howto.html response code: 404
GET https://archibus.vodacom.co.za/docs/security-howto.html response code: 404
GET https://archibus.vodacom.co.za/docs/manager-howto.html response code: 404
GET https://archibus.vodacom.co.za/manager/status response code: 404
GET https://archibus.vodacom.co.za/manager/html response code: 404
GET https://archibus.vodacom.co.za/host-manager/html response code: 404
GET https://archibus.vodacom.co.za/docs/realm-howto.html response code: 404
GET https://archibus.vodacom.co.za/docs/setup.html response code: 404
GET https://archibus.vodacom.co.za/docs/appdev/ response code: 404
GET https://archibus.vodacom.co.za/docs/changelog.html response code: 404
GET https://archibus.vodacom.co.za/docs/jndi-datasource-examples-howto.html response code: 404
GET https://archibus.vodacom.co.za/docs/RELEASE-NOTES.txt response code: 404
GET https://archibus.vodacom.co.za/docs/deployer-howto.html response code: 404
GET https://archibus.vodacom.co.za/docs/api/index.html response code: 404
GET https://archibus.vodacom.co.za/FPRWin/index.aspx response code: 401
GET https://archibus.vodacom.co.za/_Incapsula_Resource?SWKMTFSR=1&e=0.5329770916436014 response code: 200
GET https://archibus.vodacom.co.za/_Incapsula_Resource?SWKMTFSR=1&e=0.7902679497011122 response code: 200
GET https://archibus.vodacom.co.za/_Incapsula_Resource?SWKMTFSR=1&e=0.6767940789579447 response code: 200
GET https://archibus.vodacom.co.za/_Incapsula_Resource?SWKMTFSR=1&e=0.8560383602618578 response code: 200
GET https://archibus.vodacom.co.za/_Incapsula_Resource?SWKMTFSR=1&e=0.4472103130471645 response code: 200
GET https://archibus.vodacom.co.za/_Incapsula_Resource?SWKMTFSR=1&e=0.913395824408842 response code: 200
GET https://archibus.vodacom.co.za/_Incapsula_Resource?SWKMTFSR=1&e=0.4981508946970825 response code: 200
GET https://archibus.vodacom.co.za/host-manager/ response code: 404
GET https://archibus.vodacom.co.za/manager/ response code: 404
GET https://archibus.vodacom.co.za/_Incapsula_Resource?SWKMTFSR=1&e=0.7227896506086273 response code: 200
GET https://archibus.vodacom.co.za/docs/api/ response code: 404
GET https://archibus.vodacom.co.za/FPRWin/ response code: 401
GET https://archibus.vodacom.co.za/_Incapsula_Resource?CWUDNSAI=23%22xinfo=13-199918871-0%200NNN%20RT%281699815731178%202650%29%20q%280%20-1%20-1%200%29%20r%280%20-1%29%20B15%284%2c200%2c0%29%20U18%22incident_id=128000840526202745-103373459019321063 7%22edet=15%22cinfo=04000000%22rpinfo=0%22mth=GET response code: 404
GET https://archibus.vodacom.co.za/_Incapsula_Resource?CWUDNSAI=23%22xinfo=3-56251934-0%200NNN%20RT%2816919533759 15%209%29%20q%280%20-1%20-1%200%29%20r%280%20-1%29%20B15%284%2c200%2c0%29%20U18%22incident_id=451001120180377263-267491121570192387%22edet=15%22cinfo=04000000%22rpinfo=0%22mth=GET response code: 404

GET https://archibus.vodacom.co.za/_Incapsula_Resource?CWUDNSAI=23&xinfo=10-97597847-0%200NNN%20RT%281691953271388%207%29%20q%280%20-1%20-1%20-1%29%20r%280%20-1%29%20B15%284%2c200%2c0%29%20U18&incident_id=451001120180377263-45986815277656372 2&edet=15&cinfo=04000000&rpinfo=0&mth=GET response code: 200
GET https://archibus.vodacom.co.za/_Incapsula_Resource?CWUDNSAI=23%22xinfo=4-14899366-0%200NNN%20RT%281696791747744%202749%29%20q%280%20-1%20-1%200%29%20r%280%20-1%29%20B15%284%2c200%2c0%29%20U18%22incident_id=763001140096022537-78103340377644164%22edet=15%22cinfo=04000000%22rpinfo=0%22mth=GET response code: 404
GET https://archibus.vodacom.co.za/_Incapsula_Resource?CWUDNSAI=23&xinfo=11-189604665-0%200NNN%20RT%281684090921855%202362%29%20q%280%20-1%20-1%200%29%20r%280%20-1%29%20B15%284%2C200%2C0%29%20U18&incident_id=764000300423775679-91206306729689281 1&edet=15&cinfo=04000000&rpinfo=0&mth=GET response code: 200
GET https://archibus.vodacom.co.za/_Incapsula_Resource?CWUDNSAI=23&xinfo=11-217099708-0%200NNN%20RT%281688929427421%2010%29%20q%280%20-1%20-1%20-1%29%20r%280%20-1%29%20B15%284%2C200%2C0%29%20U18&incident_id=281000660478098624-104987613815852660 3&edet=15&cinfo=04000000&rpinfo=0&mth=GET response code: 200
GET https://archibus.vodacom.co.za/_Incapsula_Resource?CWUDNSAI=23%22xinfo=9-84466755-0%200NNN%20RT%281691953378741%2023202%29%20q%280%20-1%20-1%200%29%20r%280%20-1%29%20B15%284%2c200%2c0%29%20U18%22incident_id=451001120180377263-39711952669056103 3%22edet=15%22cinfo=04000000%22rpinfo=0%22mth=GET response code: 404
GET https://archibus.vodacom.co.za/_Incapsula_Resource?CWUDNSAI=23%22xinfo=9-63593046-0%200NNN%20RT%281694372516502%202831%29%20q%280%20-1%20-1%200%29%20r%280%20-1%29%20B15%284%2c200%2c0%29%20U18%22incident_id=451001150135587882-31333309852176301 7%22edet=15%22cinfo=04000000%22rpinfo=0%22mth=GET response code: 404
GET https://archibus.vodacom.co.za/_Incapsula_Resource?CWUDNSAI=23&xinfo=10-42257572-0%200NNN%20RT%281686510627231%202271%29%20q%280%20-1%20-1%200%29%20r%280%20-1%29%20B15%284%2C200%2C0%29%20U18&incident_id=767000350234861307-20730123086142074 6&edet=15&cinfo=04000000&rpinfo=0&mth=GET response code: 200
GET https://archibus.vodacom.co.za/_Incapsula_Resource?CWUDNSAI=23&xinfo=12-32525279-0%200NNN%20RT%281696791747727%209%29%20q%280%20-1%20-1%20-1%29%20r%280%20-1%29%20B15%284%2C200%2C0%29%20U18&incident_id=763001140096022537-16422554356069902 0&edet=15&cinfo=04000000&rpinfo=0&mth=GET response code: 200
GET https://archibus.vodacom.co.za/_Incapsula_Resource?CWUDNSAI=23&xinfo=12-68759309-0%200NNN%20RT%281686510514654%204%29%20q%280%20-1%20-1%20-1%29%20r%280%20-1%29%20B15%284%2c200%2c0%29%20U18&incident_id=767000350234861307-33774074485060628 4&edet=15&cinfo=04000000&rpinfo=0&mth=GET response code: 200
GET https://archibus.vodacom.co.za/_Incapsula_Resource?CWUDNSAI=23%22xinfo=4-71886990-0%200NNN%20RT%281702234922706%202787%29%20q%280%20-1%20-1%201%29%20r%280%20-1%29%20B15%284%2c200%2c0%29%20U18%22incident_id=763001220427927261-37704257323683802 0%22edet=15%22cinfo=04000000%22rpinfo=0%22mth=GET response code: 404
GET https://archibus.vodacom.co.za/_Incapsula_Resource?CWUDNSAI=23%22xinfo=42-8036113-0%200NNN%20RT%281705258980606%202800%29%20q%280%20-1%20-1%202%29%20r%280%20-1%29%20B15%284%2c200%2c0%29%20U18%22incident_id=168700006022390130 6-46148676381770154%22edet=15%22cinfo=04000000%22rpinfo=0%22mth=GET response code: 404
GET https://archibus.vodacom.co.za/_Incapsula_Resource?CWUDNSAI=23&xinfo=13-199918871-0%200NNN%20RT%281699815731178%202650%29%20q%280%20-1%20-1%200%29%20r%280%20-1%29%20B15%284%2C200%2C0%29%20U18&incident_id=128000840526202745-10337345901932106 37&edet=15&cinfo=04000000&rpinfo=0&mth=GET response code: 200
GET https://archibus.vodacom.co.za/_Incapsula_Resource?CWUDNSAI=23%22xinfo=9-142984614-0%200NNN%20RT%281688929427439%202760%29%20q%280%20-1%20-1%200%29%20r%281%20-1%29%20B15%284%2c200%2c0%29%20U18%22incident_id=281000660478098624-68876733529411188 1%22edet=15%22cinfo=04000000%22rpinfo=0%22mth=GET response code: 404
GET https://archibus.vodacom.co.za/_Incapsula_Resource?CWUDNSAI=23&xinfo=11-61474434-0%200NNN%20RT%281686510627214%209%29%20q%280%20-1%20-1%20-1%29%20r%280%20-1%29%20B15%284%2C200%2C0%29%20U18&incident_id=767000350234861307-30264044674659348 3&edet=15&cinfo=04000000&rpinfo=0&mth=GET response code: 200
GET https://archibus.vodacom.co.za/_Incapsula_Resource?CWUDNSAI=23&xinfo=11-93784308-0%200NNN%20RT%281702234859957%2012%29%20q%280%20-1%20-1%20-1%29%20r%280%20-1%29%20B15%284%2c200%2c0%29%20U18&incident_id=763001220427927261-49007319750089895 5&edet=15&cinfo=04000000&rpinfo=0&mth=GET response code: 200
GET https://archibus.vodacom.co.za/_Incapsula_Resource?CWUDNSAI=23&xinfo=12-217098056-0%200NNN%20RT%281684090921837%2011%29%20q%280%20-1%20-1%20-1%29%20r%280%20-1%29%20B15%284%2C200%2C0%29%20U18&incident_id=764000300423775679-10328184780056185 72&edet=15&cinfo=04000000&rpinfo=0&mth=GET response code: 200
GET https://archibus.vodacom.co.za/_Incapsula_Resource?CWUDNSAI=23&xinfo=14-153614192-0%200NNN%20RT%281681066840725%203%29%20q%280%20-1%20-1%20-1%29%20r%280%20-1%29%20B15%284%2c200%2c0%29%20U18&incident_id=768000300342834631-73515496210274907 0&edet=15&cinfo=04000000&rpinfo=0&mth=GET response code: 200
GET https://archibus.vodacom.co.za/_Incapsula_Resource?CWUDNSAI=23&xinfo=13-243380468-0%200NNN%20RT%281684090859136%203%29%20q%280%20-1%20-1%20-1%29%20r%280%20-1%29%20B15%284%2c200%2c0%29%20U18&incident_id=764000300423775679-11712587129083677 57&edet=15&cinfo=04000000&rpinfo=0&mth=GET response code: 200

150245 Missing header: X-Frame-Options (1)

150245 Missing header: X-Frame-Options

archibus.vodacom.co.za

Finding #	10510079	**Severity**	Information Gathered - Level 1
Unique #	b3d41fa5-8528-4067-bc8c-c6fcfc62515d		
Group	Security Weaknesses		
CWE	CWE-693	**Detection Date**	11 Feb 2024 21:02 GMT+0200
OWASP	A5 Security Misconfiguration		
WASC	WASC-15 APPLICATION MISCONFIGURATION		

Details

Threat

The X-Frame-Options header is not set in the HTTP response, meaning the page can potentially be loaded into an attacker-controlled frame. This could lead to clickjacking, where an attacker adds an invisible layer on top of the legitimate page to trick users into clicking on a malicious link or taking a harmful action.

Impact

Without an X-Frame-Options response header, clickjacking may be possible. However, if the application properly uses the Content-Security-Policy "frame-ancestors" directive, then modern web browsers would stop the page from being framed and prevent clickjacking.

Solution

The X-Frame-Options allows three values: DENY, SAMEORIGIN and ALLOW-FROM. It is recommended to use DENY, which prevents all domains from framing the page or SAMEORIGIN, which allows framing only by the same site. DENY and SAMEORGIN are supported by all browsers. Using ALLOW-FROM is not recommended because not all browsers support it.

Note: To avoid a common X-Frame-Options implementation mistake, see https://blog.qualys.com/securitylabs/2015/10/20/clickjacking-a-common-

implementation-mistake-that-can-put-your-websites-in-danger.

Results

X-Frame-Options header is missing or not set to DENY or SAMEORIGIN for the following pages:
(Only first 10 such pages are reported)

GET https://archibus.vodacom.co.za/_Incapsula_Resource?CWUDNSAI=23&xinfo=10-42257572-0%200NNN%20RT%281686510627231%202271%29%20q%280%20-1%20-1%200%29%20r%280%20-1%29%20B15%284%2C200%2C0%29%20U18&incident_id=767000350234861307-207301230861420746&edet=15&cinfo=04000000&rpinfo=0&mth=GET
Response code: 200
Response headers:
Cache-Control: no-cache, no-store
Content-Encoding: gzip
Content-Length: 3754
Content-Security-Policy-Report-Only: default-src 'self' 'unsafe-eval' 'unsafe-hashes' 'unsafe-inline' data: blob: ; form-action 'none' data: blob: ; report-uri /csp_report
Content-Type: text/html
X-Robots-Tag: noindex
Set-Cookie: visid_incap_2776849=FzwYQrB5SDmrEoE8GapjSPYZyWUAAAAAQUIPAAAAAACKSeVsUKW+PDQEFi62u5/P; HttpOnly; expires=Sun, 09-Feb-2025 22:21:11 GMT; domain=.vodacom.co.za; path=/
Set-Cookie: nlbi_2776849=2+b7ZdTvP3ssIFAPZU49BAAAAAATg/RB/1C/i+jo3xrjvYzk; domain=.vodacom.co.za; path=/
Set-Cookie: incap_ses_1687_2776849=lxYnX5C6qRDb7PgfvG1pF/YZyWUAAAAAg7Eia1/rhUGqMH+aaFiXQA==; domain=.vodacom.co.za; path=/
Set-Cookie: nlbi_2776849_2147483392=k5kLRvdgEWwS+lKAZU49BAAAAABQjiwoWlb3affAi7dkGbY0; domain=.vodacom.co.za; path=/

GET https://archibus.vodacom.co.za/_Incapsula_Resource?CWUDNSAI=23&xinfo=10-97597847-0%200NNN%20RT%281691953271388%207%29%20q%280%20-1%20-1%20-1%29%20r%280%20-1%29%20B15%284%2c200%2c0%29%20U18&incident_id=451001120180377263-459868152776563722&edet=15&cinfo=04000000&rpinfo=0&mth=GET
Response code: 200
Response headers:
Cache-Control: no-cache, no-store
Content-Encoding: gzip
Content-Length: 3756
Content-Security-Policy-Report-Only: default-src 'self' 'unsafe-eval' 'unsafe-hashes' 'unsafe-inline' data: blob: ; form-action 'none' data: blob: ; report-uri /csp_report
Content-Type: text/html
X-Robots-Tag: noindex
Set-Cookie: visid_incap_2776849=FzwYQrB5SDmrEoE8GapjSPYZyWUAAAAAQUIPAAAAAACKSeVsUKW+PDQEFi62u5/P; HttpOnly; expires=Sun, 09-Feb-2025 22:21:11 GMT; domain=.vodacom.co.za; path=/
Set-Cookie: nlbi_2776849=2+b7ZdTvP3ssIFAPZU49BAAAAAATg/RB/1C/i+jo3xrjvYzk; domain=.vodacom.co.za; path=/
Set-Cookie: incap_ses_1687_2776849=lxYnX5C6qRDb7PgfvG1pF/YZyWUAAAAAg7Eia1/rhUGqMH+aaFiXQA==; domain=.vodacom.co.za; path=/
Set-Cookie: nlbi_2776849_2147483392=k5kLRvdgEWwS+lKAZU49BAAAAABQjiwoWlb3affAi7dkGbY0; domain=.vodacom.co.za; path=/

GET https://archibus.vodacom.co.za/_Incapsula_Resource?CWUDNSAI=23&xinfo=11-189604665-0%200NNN%20RT%2816840909218555%202362%29%20q%280%20-1%20-1%200%29%20r%280%20-1%29%20B15%284%2C200%2C0%29%20U18&incident_id=764000300423775679-912063067296892811&edet=15&cinfo=04000000&rpinfo=0&mth=GET
Response code: 200
Response headers:
Cache-Control: no-cache, no-store
Content-Encoding: gzip
Content-Length: 3758
Content-Security-Policy-Report-Only: default-src 'self' 'unsafe-eval' 'unsafe-hashes' 'unsafe-inline' data: blob: ; form-action 'none' data: blob: ; report-uri /csp_report
Content-Type: text/html
X-Robots-Tag: noindex
Set-Cookie: visid_incap_2776849=FzwYQrB5SDmrEoE8GapjSPYZyWUAAAAAQUIPAAAAAACKSeVsUKW+PDQEFi62u5/P; HttpOnly; expires=Sun, 09-Feb-2025 22:21:11 GMT; domain=.vodacom.co.za; path=/
Set-Cookie: nlbi_2776849=2+b7ZdTvP3ssIFAPZU49BAAAAAATg/RB/1C/i+jo3xrjvYzk; domain=.vodacom.co.za; path=/
Set-Cookie: incap_ses_1687_2776849=lxYnX5C6qRDb7PgfvG1pF/YZyWUAAAAAg7Eia1/rhUGqMH+aaFiXQA==; domain=.vodacom.co.za; path=/
Set-Cookie: nlbi_2776849_2147483392=k5kLRvdgEWwS+lKAZU49BAAAAABQjiwoWlb3affAi7dkGbY0; domain=.vodacom.co.za; path=/

GET https://archibus.vodacom.co.za/_Incapsula_Resource?CWUDNSAI=23&xinfo=11-217099708-0%200NNN%20RT%2816888929427421%2010%29%20q%280%20-1%20-1%20-1%29%20r%280%20-1%29%20B15%284%2C200%2C0%29%20U18&incident_id=281000660478098624-104987613815852660 3&edet=15&cinfo=04000000&rpinfo=0&mth=GET
Response code: 200
Response headers:
Cache-Control: no-cache, no-store
Content-Encoding: gzip
Content-Length: 3757
Content-Security-Policy-Report-Only: default-src 'self' 'unsafe-eval' 'unsafe-hashes' 'unsafe-inline' data: blob: ; form-action 'none' data: blob: ; report-uri /csp_report
Content-Type: text/html
X-Robots-Tag: noindex
Set-Cookie: visid_incap_2776849=FzwYQrB5SDmrEoE8GapjSPYZyWUAAAAAQUIPAAAAAACKSeVsUKW+PDQEFi62u5/P; HttpOnly; expires=Sun, 09-Feb-2025 22:21:11 GMT; domain=.vodacom.co.za; path=/
Set-Cookie: nlbi_2776849=2+b7ZdTvP3ssIFAPZU49BAAAAAATg/RB/1C/i+jo3xrjvYzk; domain=.vodacom.co.za; path=/
Set-Cookie: incap_ses_1687_2776849=lxYnX5C6qRDb7PgfvG1pF/YZyWUAAAAAg7Eia1/rhUGqMH+aaFiXQA==; domain=.vodacom.co.za; path=/
Set-Cookie: nlbi_2776849_2147483392=k5kLRvdgEWwS+lKAZU49BAAAAABQjiwoWlb3affAi7dkGbY0; domain=.vodacom.co.za; path=/

GET https://archibus.vodacom.co.za/_Incapsula_Resource?CWUDNSAI=23&xinfo=11-61474434-0%200NNN%20RT%281686510627214%209%29%20q%280%20-1%20-1%20-1%29%20r%280%20-1%29%20B15%284%2C200%2C0%29%20U18&incident_id=767000350234861307-302640446746593483&edet=15&cinfo=04000000&rpinfo=0&mth=GET
Response code: 200
Response headers:
Cache-Control: no-cache, no-store
Content-Encoding: gzip
Content-Length: 3756
Content-Security-Policy-Report-Only: default-src 'self' 'unsafe-eval' 'unsafe-hashes' 'unsafe-inline' data: blob: ; form-action 'none' data: blob: ; report-uri /csp_report

Content-Type: text/html
X-Robots-Tag: noindex
Set-Cookie: visid_incap_2776849=FzwYQrB5SDmrEoE8GapjSPYZyWUAAAAAQUIPAAAAAACKSeVsUKW+PDQEFi62u5/P; HttpOnly; expires=Sun, 09-Feb-2025 22:21:11 GMT; domain=.vodacom.co.za; path=/
Set-Cookie: nlbi_2776849=2+b7ZdTvP3ssIFAPZU49BAAAAAATg/RB/1C/i+jo3xrjvYzk; domain=.vodacom.co.za; path=/
Set-Cookie: incap_ses_1687_2776849=lxYnX5C6qRDb7PgfvG1pF/YZyWUAAAAAg7Eia1/rhUGqMH+aaFiXQA==; domain=.vodacom.co.za; path=/
Set-Cookie: nlbi_2776849_2147483392=k5kLRvdgEWwS+lKAZU49BAAAAABQjiwoWlb3affAi7dkGbY0; domain=.vodacom.co.za; path=/

GET https://archibus.vodacom.co.za/_Incapsula_Resource?CWUDNSAI=23&xinfo=11-93784308-0%200NNN%20RT%281702234859957%2012%29%20q%280%20-1%20-1%20-1%29%20r%280%20-1%29%20B15%284%2c200%2c0%29%20U18&incident_id=763001220427927261-49007319750089895 5&edet=15&cinfo=04000000&rpinfo=0&mth=GET
Response code: 200
Response headers:
Cache-Control: no-cache, no-store
Content-Encoding: gzip
Content-Length: 3759
Content-Security-Policy-Report-Only: default-src 'self' 'unsafe-eval' 'unsafe-hashes' 'unsafe-inline' data: blob: ; form-action 'none' data: blob: ; report-uri /csp_report
Content-Type: text/html
X-Robots-Tag: noindex
Set-Cookie: visid_incap_2776849=FzwYQrB5SDmrEoE8GapjSPYZyWUAAAAAQUIPAAAAAACKSeVsUKW+PDQEFi62u5/P; HttpOnly; expires=Sun, 09-Feb-2025 22:21:11 GMT; domain=.vodacom.co.za; path=/
Set-Cookie: nlbi_2776849=2+b7ZdTvP3ssIFAPZU49BAAAAAATg/RB/1C/i+jo3xrjvYzk; domain=.vodacom.co.za; path=/
Set-Cookie: incap_ses_1687_2776849=lxYnX5C6qRDb7PgfvG1pF/YZyWUAAAAAg7Eia1/rhUGqMH+aaFiXQA==; domain=.vodacom.co.za; path=/
Set-Cookie: nlbi_2776849_2147483392=k5kLRvdgEWwS+lKAZU49BAAAAABQjiwoWlb3affAi7dkGbY0; domain=.vodacom.co.za; path=/

GET https://archibus.vodacom.co.za/_Incapsula_Resource?CWUDNSAI=23&xinfo=12-217098056-0%200NNN%20RT%2816840909218 37%2011%29%20q%280%20-1%20-1%20-1%29%20r%280%20-1%29%20B15%284%2C200%2C0%29%20U18&incident_id=764000300423775679-103281847800561 8572&edet=15&cinfo=04000000&rpinfo=0&mth=GET
Response code: 200
Response headers:
Cache-Control: no-cache, no-store
Content-Encoding: gzip
Content-Length: 3757
Content-Security-Policy-Report-Only: default-src 'self' 'unsafe-eval' 'unsafe-hashes' 'unsafe-inline' data: blob: ; form-action 'none' data: blob: ; report-uri /csp_report
Content-Type: text/html
X-Robots-Tag: noindex
Set-Cookie: visid_incap_2776849=FzwYQrB5SDmrEoE8GapjSPYZyWUAAAAAQUIPAAAAAACKSeVsUKW+PDQEFi62u5/P; HttpOnly; expires=Sun, 09-Feb-2025 22:21:11 GMT; domain=.vodacom.co.za; path=/
Set-Cookie: nlbi_2776849=2+b7ZdTvP3ssIFAPZU49BAAAAAATg/RB/1C/i+jo3xrjvYzk; domain=.vodacom.co.za; path=/
Set-Cookie: incap_ses_1687_2776849=lxYnX5C6qRDb7PgfvG1pF/YZyWUAAAAAg7Eia1/rhUGqMH+aaFiXQA==; domain=.vodacom.co.za; path=/
Set-Cookie: nlbi_2776849_2147483392=k5kLRvdgEWwS+lKAZU49BAAAAABQjiwoWlb3affAi7dkGbY0; domain=.vodacom.co.za; path=/

GET https://archibus.vodacom.co.za/_Incapsula_Resource?CWUDNSAI=23&xinfo=12-32525279-0%200NNN%20RT%281696791747727%209%29%20q%280%20-1%20-1%20-1%29%20r%280%20-1%29%20B15%284%2C200%2C0%29%20U18&incident_id=763001140096022537-164225543560699020&edet=15&cinfo=04000000&rpinfo=0&mth=GET
Response code: 200
Response headers:
Cache-Control: no-cache, no-store
Content-Encoding: gzip
Content-Length: 3755
Content-Security-Policy-Report-Only: default-src 'self' 'unsafe-eval' 'unsafe-hashes' 'unsafe-inline' data: blob: ; form-action 'none' data: blob: ; report-uri /csp_report
Content-Type: text/html
X-Robots-Tag: noindex
Set-Cookie: visid_incap_2776849=FzwYQrB5SDmrEoE8GapjSPYZyWUAAAAAQUIPAAAAAACKSeVsUKW+PDQEFi62u5/P; HttpOnly; expires=Sun, 09-Feb-2025 22:21:11 GMT; domain=.vodacom.co.za; path=/
Set-Cookie: nlbi_2776849=2+b7ZdTvP3ssIFAPZU49BAAAAAATg/RB/1C/i+jo3xrjvYzk; domain=.vodacom.co.za; path=/
Set-Cookie: incap_ses_1687_2776849=lxYnX5C6qRDb7PgfvG1pF/YZyWUAAAAAg7Eia1/rhUGqMH+aaFiXQA==; domain=.vodacom.co.za; path=/
Set-Cookie: nlbi_2776849_2147483392=k5kLRvdgEWwS+lKAZU49BAAAAABQjiwoWlb3affAi7dkGbY0; domain=.vodacom.co.za; path=/

GET https://archibus.vodacom.co.za/_Incapsula_Resource?CWUDNSAI=23&xinfo=12-68759309-0%200NNN%20RT%281686510514654%204%29%20q%280%20-1%20-1%20-1%29%20r%280%20-1%29%20B15%284%2c200%2c0%29%20U18&incident_id=767000350234861307-337740744850606284&edet=15&cinfo=04000000&rpinfo=0&mth=GET
Response code: 200
Response headers:
Cache-Control: no-cache, no-store
Content-Encoding: gzip
Content-Length: 3758
Content-Security-Policy-Report-Only: default-src 'self' 'unsafe-eval' 'unsafe-hashes' 'unsafe-inline' data: blob: ; form-action 'none' data: blob: ; report-uri /csp_report
Content-Type: text/html
X-Robots-Tag: noindex
Set-Cookie: visid_incap_2776849=FzwYQrB5SDmrEoE8GapjSPYZyWUAAAAAQUIPAAAAAACKSeVsUKW+PDQEFi62u5/P; HttpOnly; expires=Sun, 09-Feb-2025 22:21:11 GMT; domain=.vodacom.co.za; path=/
Set-Cookie: nlbi_2776849=2+b7ZdTvP3ssIFAPZU49BAAAAAATg/RB/1C/i+jo3xrjvYzk; domain=.vodacom.co.za; path=/
Set-Cookie: incap_ses_1687_2776849=lxYnX5C6qRDb7PgfvG1pF/YZyWUAAAAAg7Eia1/rhUGqMH+aaFiXQA==; domain=.vodacom.co.za; path=/
Set-Cookie: nlbi_2776849_2147483392=k5kLRvdgEWwS+lKAZU49BAAAAABQjiwoWlb3affAi7dkGbY0; domain=.vodacom.co.za; path=/

GET https://archibus.vodacom.co.za/_Incapsula_Resource?CWUDNSAI=23&xinfo=13-199918871-0%200NNN%20RT%2816998157311 78%202650%29%20q%280%20-1%20-1%200%29%20r%280%20-1%29%20B15%284%2C200%2C0%29%20U18&incident_id=128000840526202745-10337345901932106 37&edet=15&cinfo=04000000&rpinfo=0&mth=GET
Response code: 200
Response headers:
Cache-Control: no-cache, no-store
Content-Encoding: gzip
Content-Length: 3757
Content-Security-Policy-Report-Only: default-src 'self' 'unsafe-eval' 'unsafe-hashes' 'unsafe-inline' data: blob: ; form-action 'none' data: blob: ; report-uri /csp_report
Content-Type: text/html
X-Robots-Tag: noindex
Set-Cookie: visid_incap_2776849=FzwYQrB5SDmrEoE8GapjSPYZyWUAAAAAQUIPAAAAAACKSeVsUKW+PDQEFi62u5/P; HttpOnly; expires=Sun, 09-Feb-2025 22:21:11 GMT; domain=.vodacom.co.za; path=/
Set-Cookie: nlbi_2776849=2+b7ZdTvP3ssIFAPZU49BAAAAAATg/RB/1C/i+jo3xrjvYzk; domain=.vodacom.co.za; path=/

Set-Cookie: incap_ses_1687_2776849=lxYnX5C6qRDb7PgfvG1pF/YZyWUAAAAAg7Eia1/rhUGqMH+aaFiXQA==; domain=.vodacom.co.za; path=/
Set-Cookie: nlbi_2776849_2147483392=k5kLRvdgEWwS+lKAZU49BAAAAABQjiwoWlb3affAi7dkGbY0; domain=.vodacom.co.za; path=/

150277 Cookie without SameSite attribute (1)

150277 Cookie without SameSite attribute — archibus.vodacom.co.za

Finding #	10510080	**Severity**	Information Gathered - Level 1
Unique #	8187888e-a07a-473f-938e-a821fe364035		
Group	Security Weaknesses		
CWE	CWE-16, CWE-1032	**Detection Date**	11 Feb 2024 21:02 GMT+0200
OWASP	A5 Security Misconfiguration		
WASC	-		

Details

Threat
The cookies listed in the Results section are missing the SameSite attribute.

Impact
The SameSite cookie attribute is an effective countermeasure against cross-site request forgery (CSRF) attacks. Note that a missing SameSite attribute does not mean the web application is automatically vulnerable to CSRF. The scanner will report QID 150071 if a CSRF vulnerability is detected.

Solution
Consider adding the SameSite attribute to the cookie(s) listed.

More information:
DZone article
OWASP CSRF Prevention Cheat Sheet

Results

Total cookies: 4
incap_ses_1687_2776849=lxYnX5C6qRDb7PgfvG1pF/YZyWUAAAAAg7Eia1/rhUGqMH+aaFiXQA==; path=/; domain=.vodacom.co.za | First set at URL: https://archibus.vodacom.co.za/
nlbi_2776849=2+b7ZdTvP3ssIFAPZU49BAAAAAATg/RB/1C/i+jo3xrjvYzk; path=/; domain=.vodacom.co.za | First set at URL: https://archibus.vodacom.co.za/
nlbi_2776849_2147483392=WoCbbZ/T0xODuuO8ZU49BAAAAAC4rTMSqcwSp5j8m2+NYJTV; path=/; domain=.vodacom.co.za | First set at URL: https://archibus.vodacom.co.za/
visid_incap_2776849=FzwYQrB5SDmrEoE8GapjSPYZyWUAAAAAQUIPAAAAAACKSeVsUKW+PDQEFi62u5/P; expires=Sun Feb 9 22:21:11 2025; path=/; domain=.vodacom.co.za; max-age=31459842; httponly | First set at URL: https://archibus.vodacom.co.za/

archibus.vodacom.co.za/archibus/ (61)

Vulnerability (18)

Cross-Site Scripting (1)

150541 Apache Tomcat Cross-Site Scripting(XSS) Vulnerability (CVE-2022-34305) (1)

150541 Apache Tomcat Cross-Site Scripting(XSS) Vulnerability (CVE-2022-34305) — archibus.vodacom.co.za/archibus/ New

URL: https://archibus.vodacom.co.za/BTUJ121J.1tmhl

Finding #	23859792	**Severity**	Potential Vulnerability - Level 3
Unique #	4c742d2e-057b-43f9-9951-b99a09d7e854		
Group	Cross-Site Scripting	**First Time Detected**	11 Feb 2024 21:02 GMT+0200
CWE	CWE-79	**Last Time Detected**	11 Feb 2024 21:02 GMT+0200
OWASP	A3 Injection	**Last Time Tested**	11 Feb 2024 21:02 GMT+0200
WASC	WASC-8 CROSS-SITE SCRIPTING	**Times Detected**	1

WAS Web Application Report

CVSS V3 Base	6.1	**CVSS V3 Temporal**	5.3	**CVSS V3 Attack Vector**	Network

Details

Threat

Apache Tomcat is an open source web server and servlet container developed by the Apache Software Foundation.

In affected versions of Apache Tomcat, the Form authentication example in the examples web application displayed user provided data without filtering, exposing a XSS vulnerability.

Affected Versions:
Apache Tomcat 10.1.0-M1 to 10.1.0-M16
Apache Tomcat 10.0.0-M1 to 10.0.22
Apache Tomcat 9.0.30 to 9.0.64
Apache Tomcat 8.5.50 to 8.5.81

QID Detection Logic (Unauthenticated):
This QID sends a HTTP GET request to a invalid URL and based on the response confirms the vulnerable instance of Apache Tomcat running on the host.

Impact

Successful exploitation could allow an attacker to execute arbitrary JavaScript code in the context of the interface or allow the attacker to access sensitive, browser-based information.

Solution

Customers are advised to upgrade Apache Tomcat to new version to remediate this vulnerability. For more information please refer to Apache Tomcat Security Advisory.

Detection Information

Parameter	No param has been required for detecting the information.
Authentication	In order to detect this vulnerability, no authentication has been required.

Payloads

#1 Request

GET https://archibus.vodacom.co.za/BTUJ121J.1tmhl

Referer: https://archibus.vodacom.co.za/archibus/
Cookie: visid_incap_2776849=h50ySIBaTWWx5gCZcxRDIlQryWUAAAAAQUIPAAAAAACcSzBMcBx1U7rC3oommybq;
incap_ses_1687_2776849=il3uMHuTAW0RdhIgvG1pF1QryWUAAAAAci4S6kd04giEDL+dpN7m+w==;
Host: archibus.vodacom.co.za
User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/102.0.5005.177 Safari/537.36
Accept: */*

Click this link to try to reproduce the vulnerability using above payload.Note that clicking this link may not lead to visible results, either because the vulnerability requires context to be previously set (authentication, cookies...) or because the exploitation of the vulnerability does not lead to any visible proof.

#1 Response

comment: Apache Tomcat Cross-Site Scripting(XSS) Vulnerability (CVE-2022-34305) found at PORT : 443

he requested resource [/BTUJ121J.1tmhl] is not available Description The origin server did not find a current representation for the target resource or is not willing to disclose that one exists. <hr class="line" /><h3>Apache Tomcat/9.0.62</h3><script type="text/javascript" src="/_Incapsula_Resource?SWJIYLWA=719d34d31c8e3a6e6fffd425f7e032f3&ns=1&cb=1614654173" async></script></body></html>

* The reflected string on the response webpage indicates that the vulnerability test was successful

WAS Web Application Report

Information Disclosure (17)

150531 Apache Tomcat EncryptInterceptor DoS Vulnerability (CVE-2022-29885) (1)

150531 Apache Tomcat EncryptInterceptor DoS Vulnerability (CVE-2022-29885) *archibus.vodacom.co.za/archibus/* **New**

URL: https://archibus.vodacom.co.za/OEO3mB20.1tmhl

Finding #	23859794	**Severity**	Potential Vulnerability - Level 4
Unique #	868ed53b-89b0-4341-a1bd-b17e6faad0b4		
Group	Information Disclosure	**First Time Detected**	11 Feb 2024 21:02 GMT+0200
CWE	CWE-400	**Last Time Detected**	11 Feb 2024 21:02 GMT+0200
OWASP	A6 Vulnerable and Outdated Components	**Last Time Tested**	11 Feb 2024 21:02 GMT+0200
WASC	WASC-10 DENIAL OF SERVICE	**Times Detected**	1

CVSS V3 Base 7.5 **CVSS V3 Temporal** 6.7 **CVSS V3 Attack Vector** Network

Details

Threat

Apache Tomcat is an open source web server and servlet container developed by the Apache Software Foundation.

In affected versions of Apache Tomcat, the documentation for the EncryptInterceptor incorrectly stated it enabled Tomcat clustering to run over an untrusted network. This was not correct. While the EncryptInterceptor does provide confidentiality and integrity protection, it does not protect against all risks associated with running over any untrusted network, particularly DoS risks.

Affected Versions:
Apache Tomcat 10.1.0-M1 to 10.1.0-M14
Apache Tomcat 10.0.0-M1 to 10.0.20
Apache Tomcat 9.0.13 to 9.0.62
Apache Tomcat 8.5.38 to 8.5.78

QID Detection Logic (Unauthenticated):
This QID sends a HTTP GET request to a invalid URL and based on the response confirms the vulnerable instance of Apache Tomcat running on the host.

Impact

Successful exploitation of the vulnerability can allow an attacker to trigger a DoS via an Uncontrolled Resource Consumption

Solution

Upgrade to the Apache Tomcat to the latest version of Apache Tomcat. Please refer to Apache Tomcat Security Advisory.

Detection Information

Parameter	No param has been required for detecting the information.
Authentication	In order to detect this vulnerability, no authentication has been required.

Payloads

#1 Request

GET https://archibus.vodacom.co.za/OEO3mB20.1tmhl

Referer: https://archibus.vodacom.co.za/archibus/
Cookie: visid_incap_2776849=/6V8jlgvS2ijlJ4cTn1HhFMryWUAAAAAQUIPAAAAAAByL2AsOiragH/29B8AD5OZ;
incap_ses_1687_2776849=Z6L4OrXms1NqdBIgvG1pF1MryWUAAAAA2ZjoCsm4XnOVUQB4Fvhd8g==;
Host: archibus.vodacom.co.za
User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/102.0.5005.177 Safari/537.36
Accept: */*

Click this link to try to reproduce the vulnerability using above payload.Note that clicking this link may not lead to visible results, either because the vulnerability requires context to be previously set (authentication, cookies...) or because the exploitation of the vulnerability does not lead to any visible proof.

#1 Response

comment: Apache Tomcat EncryptInterceptor DoS Vulnerability (CVE-2022-29885) found at PORT : 443

he requested resource [/OEO3mB20.1tmhl] is not available Description The origin server did not find a current representation for the target resource or is not willing to disclose that one exists. <hr class="line" /><h3>Apache Tomcat/9.0.62</h3><script type="text/javascript" src="/_Incapsula_Resource?SWJIYLWA=719d34d31c8e3a6e6fffd425f7e032f3&ns=1&cb=2071279033" async></script></body></html>

* The reflected string on the response webpage indicates that the vulnerability test was successful

150590 Apache Tomcat HTTP Request Smuggling Vulnerability (CVE-2022-42252) (1)

150590 Apache Tomcat HTTP Request Smuggling Vulnerability (CVE-2022-42252)

archibus.vodacom.co.za/archibus/ **New**

URL: https://archibus.vodacom.co.za/60g3PIUD.1tmhl

Finding #	23859790	**Severity**	Potential Vulnerability - Level 4
Unique #	f33e9465-b2ce-4bd5-a216-1225caf0c079		
Group	Information Disclosure	**First Time Detected**	11 Feb 2024 21:02 GMT+0200
CWE	CWE-20, CWE-444	**Last Time Detected**	11 Feb 2024 21:02 GMT+0200
OWASP	A4 Insecure Design	**Last Time Tested**	11 Feb 2024 21:02 GMT+0200
WASC	WASC-26 HTTP REQUEST SMUGGLING	**Times Detected**	1

CVSS V3 Base	7.5	**CVSS V3 Temporal**	6.5	**CVSS V3 Attack Vector**	Network

Details

Threat

Apache Tomcat is an open source web server and servlet container developed by the Apache Software Foundation.

If Tomcat was configured to ignore invalid HTTP headers via setting rejectIllegalHeader to false (not the default), Tomcat did not reject a request containing an invalid Content-Length header making a request smuggling attack possible if Tomcat was located behind a reverse proxy that also failed to reject the request with the invalid header.

Affected Versions:
Apache Tomcat 10.1.0-M1 to 10.1.0
Apache Tomcat 10.0.0-M1 to 10.0.26
Apache Tomcat 9.0.0-M1 to 9.0.67
Apache Tomcat 8.5.0 to 8.5.52

QID Detection Logic (Unauthenticated):
This QID sends a HTTP GET request to a invalid URL and based on the response confirms the vulnerable instance of Apache Tomcat running on the host.

Impact

Exploitation of the vulnerability could lead to HTTP request smuggling attack.

Solution

Customers are advised to upgrade Apache Tomcat to new version to remediate this vulnerability. For more information please refer to Apache Tomcat Security Advisory.

Detection Information

Parameter	No param has been required for detecting the information.
Authentication	In order to detect this vulnerability, no authentication has been required.

Payloads

#1 Request

GET https://archibus.vodacom.co.za/60g3PIUD.1tmhl

Referer: https://archibus.vodacom.co.za/archibus/
Cookie: visid_incap_2776849=B12j2O6KSRiGOyjqmVX4PI8ryWUAAAAAQUIPAAAAAADOQpDoT4oF44pshIvBmQZ2;
incap_ses_1687_2776849=lWjVXQNTbEoC0BIgvG1pF48ryWUAAAAA0MLvyKT9tqmTS5XME9hztg==;
Host: archibus.vodacom.co.za
User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/102.0.5005.177 Safari/537.36
Accept: */*

Click this link to try to reproduce the vulnerability using above payload.Note that clicking this link may not lead to visible results, either because the vulnerability requires context to be previously set (authentication, cookies...) or because the exploitation of the vulnerability does not lead to any visible proof.

#1 Response

comment: Apache Tomcat HTTP Request Smuggling Vulnerability (CVE-2022-42252) found at PORT : 443

he requested resource [/60g3PIUD.1tmhl] is not available Description The origin server did not find a current representation for the target resource or is not willing to disclose that one exists. <hr class="line" /><h3>Apache Tomcat/9.0.62</h3><script type="text/javascript" src="/_Incapsula_Resource?SWJIYLWA=719d34d31c8e3a6e6fffd425f7e032f3&ns=1&cb=388493342" async></script></body></html>

* The reflected string on the response webpage indicates that the vulnerability test was successful

150755 Apache Tomcat Request Smuggling Vulnerability (CVE-2023-46589) (1)

150755 Apache Tomcat Request Smuggling Vulnerability (CVE-2023-46589) — *archibus.vodacom.co.za/archibus/* **New**

URL: https://archibus.vodacom.co.za/fGEFio2S.1tmhl

Finding #	23859780	**Severity**	Potential Vulnerability - Level 4
Unique #	fb87c9d3-c385-4deb-b0f8-a3cae11d8217		
Group	Information Disclosure	**First Time Detected**	11 Feb 2024 21:02 GMT+0200
CWE	CWE-444	**Last Time Detected**	11 Feb 2024 21:02 GMT+0200
OWASP	A4 Insecure Design	**Last Time Tested**	11 Feb 2024 21:02 GMT+0200
WASC	WASC-26 HTTP REQUEST SMUGGLING	**Times Detected**	1

CVSS V3 Base 7.5 **CVSS V3 Temporal** 6.5 **CVSS V3 Attack Vector** Network

Details

Threat

Apache Tomcat is an open source web server and servlet container developed by the Apache Software Foundation.

Tomcat did not correctly parse HTTP trailer headers. A specially crafted trailer header that exceeded the header size limit could cause Tomcat to treat a single request as multiple requests leading to the possibility of request smuggling when behind a reverse proxy.

Affected Versions:
Apache Tomcat 11.0.0-M1 to 11.0.0-M10
Apache Tomcat 10.1.0-M1 to 10.1.15
Apache Tomcat 9.0.0-M1 to 9.0.82
Apache Tomcat 8.5.0 to 8.5.95

QID Detection Logic (Unauthenticated):
This QID sends a HTTP GET request to a invalid URL and based on the response confirms the vulnerable instance of Apache Tomcat running on the host.

Impact
Exploitation of the vulnerability could lead to HTTP request smuggling attack.

Solution
Customers are advised to upgrade relevant versions of Apache Tomcat:
Apache Tomcat 11.0.0-M11 or later
Apache Tomcat 10.1.16 or later
Apache Tomcat 9.0.83 or later
Apache Tomcat 8.5.96 or later
For more information on this vulnerability please refer Apache Tomcat 8 Security Advisory, Apache Tomcat 9 Security Advisory, Apache Tomcat 10 Security Advisory, Apache Tomcat 11 Security Advisory.

Detection Information

Parameter	No param has been required for detecting the information.
Authentication	In order to detect this vulnerability, no authentication has been required.

Payloads

#1 Request

GET https://archibus.vodacom.co.za/fGEFio2S.1tmhl

Referer: https://archibus.vodacom.co.za/archibus/
Cookie: visid_incap_2776849=uRvJ3AXlQJG+8IE+AUf+qF0tyWUAAAAAQUIPAAAAAADvNYDyqFIaXSw/VgFRAIDR; incap_ses_1687_2776849=RnJ/KqyqqCwHlhUgvG1pF10tyWUAAAAAAfCLE49aKNgLxnKR4bDpJw==;
Host: archibus.vodacom.co.za
User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/102.0.5005.177 Safari/537.36
Accept: */*

Click this link to try to reproduce the vulnerability using above payload.Note that clicking this link may not lead to visible results, either because the vulnerability requires context to be previously set (authentication, cookies...) or because the exploitation of the vulnerability does not lead to any visible proof.

#1 Response

comment: Apache Tomcat Request Smuggling Vulnerability (CVE-2023-46589) found at PORT : 443

he requested resource [/fGEFio2S.1tmhl] is not available Description The origin server did not find a current representation for the target resource or is not willing to disclose that one exists. <hr class="line" /><h3>Apache Tomcat/9.0.62</h3><script type="text/javascript" src="/_Incapsula_Resource?SWJIYLWA=719d34d31c8e3a6e6fffd425f7e032f3&ns=1&cb=1159032404" async></script></body></html>

* The reflected string on the response webpage indicates that the vulnerability test was successful

150124 Clickjacking - Framable Page (3)

150124 Clickjacking - Framable Page — *archibus.vodacom.co.za/archibus/* **Active**

URL: https://archibus.vodacom.co.za/_Incapsula_Resource?CWUDNSAI=23%26xinfo=5-50820854-0%200NNN%20RT%281679264255462%2015893%29%20q%280%20-1%20-1%200%29%20r%280%20-1%29%20B15%284%2C200%2C0%29%20U18%26incident_id=770000900199789309-246450605088970373%26edet=15%26cinfo=04000000%26rpinfo=0%26mth=GET

Finding #	18390814	**Severity**	Confirmed Vulnerability - Level 3

WAS Web Application Report

Unique #	18d7f7ef-3298-4f95-94e7-7a8145ae13d5		
Group	Information Disclosure	**First Time Detected**	22 Jan 2023 21:27 GMT+0200
CWE	CWE-451	**Last Time Detected**	11 Feb 2024 21:02 GMT+0200
OWASP	A5 Security Misconfiguration	**Last Time Tested**	11 Feb 2024 21:02 GMT+0200
WASC	WASC-15 APPLICATION MISCONFIGURATION	**Times Detected**	15

CVSS V3 Base 5.8 **CVSS V3 Temporal** 5.5 **CVSS V3 Attack Vector** Network

Details

Threat

The web page can be framed. This means that clickjacking attacks against users are possible.
Note: Only 10 pages are reported for this QID similar to 150245 Missing header: X-Frame-Options

Impact

With clickjacking, an attacker can trick a victim user into clicking an invisible frame on the web page, thereby causing the victim to take an action they did not intend to take.

Solution

Clickjacking prevention mechanisms include:
- X-Frame-Options: This HTTP response header can be used to prevent framing of web pages.
- Content-Security-Policy: The 'frame-ancestors' directive can be used to prevent framing of web pages.
- Framekiller JavaScript code designed to prevent a malicious user from framing the page. This method is not recommended due to its unreliability.

See the OWASP Clickjacking Defense Cheat Sheet for more information.
To avoid a common X-Frame-Options implementation mistake, see https://blog.qualys.com/securitylabs/2015/10/20/clickjacking-a-common-implementation-mistake-that-can-put-your-websites-in-danger.

Detection Information

Parameter	No param has been required for detecting the information.
Authentication	In order to detect this vulnerability, no authentication has been required.

Payloads

#1 Request

GET https://archibus.vodacom.co.za/_Incapsula_Resource?CWUDNSAI=23&xinfo=5-50820 854-0%200NNN%20RT%281679264255462%2015893%29%20q%280%20-1%20-1%200%29%20r%280%20 -1%29%20B15%284%2C200%2C0%29%20U18&incident_id=770000900199789309-2464506050 88970373&edet=15&cinfo=04000000&rpinfo=0&mth=GET

Host: archibus.vodacom.co.za
User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/102.0.5005.177 Safari/537.36
Accept: */*

Click this link to try to reproduce the vulnerability using above payload.Note that clicking this link may not lead to visible results, either because the vulnerability requires context to be previously set (authentication, cookies...) or because the exploitation of the vulnerability does not lead to any visible proof.

#1 Response

The URI was framed.

150124 Clickjacking - Framable Page

archibus.vodacom.co.za/archibus/ **New**

URL: https://archibus.vodacom.co.za/_Incapsula_Resource?SWKMTFSR=1%26e=0.748959364503075

Finding #	23859804	**Severity**	Confirmed Vulnerability - Level 3
Unique #	378f66cf-daee-4b7f-9029-5a0940b206c5		
Group	Information Disclosure	**First Time Detected**	11 Feb 2024 21:02 GMT+0200

WAS Web Application Report

CWE	CWE-451	Last Time Detected	11 Feb 2024 21:02 GMT+0200
OWASP	A5 Security Misconfiguration	Last Time Tested	11 Feb 2024 21:02 GMT+0200
WASC	WASC-15 APPLICATION MISCONFIGURATION	Times Detected	1

CVSS V3 Base	5.8	CVSS V3 Temporal	5.5	CVSS V3 Attack Vector	Network

Details

Threat

The web page can be framed. This means that clickjacking attacks against users are possible.
Note: Only 10 pages are reported for this QID similar to 150245 Missing header: X-Frame-Options

Impact

With clickjacking, an attacker can trick a victim user into clicking an invisible frame on the web page, thereby causing the victim to take an action they did not intend to take.

Solution

Clickjacking prevention mechanisms include:
- X-Frame-Options: This HTTP response header can be used to prevent framing of web pages.
- Content-Security-Policy: The 'frame-ancestors' directive can be used to prevent framing of web pages.
- Framekiller JavaScript code designed to prevent a malicious user from framing the page. This method is not recommended due to its unreliability.

See the OWASP Clickjacking Defense Cheat Sheet for more information.
To avoid a common X-Frame-Options implementation mistake, see https://blog.qualys.com/securitylabs/2015/10/20/clickjacking-a-common-implementation-mistake-that-can-put-your-websites-in-danger.

Detection Information

Parameter	No param has been required for detecting the information.
Authentication	In order to detect this vulnerability, no authentication has been required.
Access Path	Here is the path followed by the scanner to reach the exploitable URL:

https://archibus.vodacom.co.za/archibus/
https://archibus.vodacom.co.za/
https://archibus.vodacom.co.za/manager/status

Payloads

#1 Request

GET https://archibus.vodacom.co.za/_Incapsula_Resource?SWKMTFSR=1&e=0.3450785737 536535
Host: archibus.vodacom.co.za
User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/102.0.5005.177 Safari/537.36
Accept: */*

Click this link to try to reproduce the vulnerability using above payload.Note that clicking this link may not lead to visible results, either because the vulnerability requires context to be previously set (authentication, cookies...) or because the exploitation of the vulnerability does not lead to any visible proof.

#1 Response

The URI was framed.

150124 Clickjacking - Framable Page — *archibus.vodacom.co.za/archibus/* **New**

URL: https://archibus.vodacom.co.za/favicon.ico

Finding #	23859800	Severity	Confirmed Vulnerability - Level 3
Unique #	cf73e484-08ea-4851-bead-451bc5024999		

WAS Web Application Report

Group	Information Disclosure	**First Time Detected**	11 Feb 2024 21:02 GMT+0200
CWE	CWE-451	**Last Time Detected**	11 Feb 2024 21:02 GMT+0200
OWASP	A5 Security Misconfiguration	**Last Time Tested**	11 Feb 2024 21:02 GMT+0200
WASC	WASC-15 APPLICATION MISCONFIGURATION	**Times Detected**	1

CVSS V3 Base 5.8 **CVSS V3 Temporal** 5.5 **CVSS V3 Attack Vector** Network

Details

Threat

The web page can be framed. This means that clickjacking attacks against users are possible.
Note: Only 10 pages are reported for this QID similar to 150245 Missing header: X-Frame-Options

Impact

With clickjacking, an attacker can trick a victim user into clicking an invisible frame on the web page, thereby causing the victim to take an action they did not intend to take.

Solution

Clickjacking prevention mechanisms include:
- X-Frame-Options: This HTTP response header can be used to prevent framing of web pages.
- Content-Security-Policy: The 'frame-ancestors' directive can be used to prevent framing of web pages.
- Framekiller JavaScript code designed to prevent a malicious user from framing the page. This method is not recommended due to its unreliability.

See the OWASP Clickjacking Defense Cheat Sheet for more information.
To avoid a common X-Frame-Options implementation mistake, see https://blog.qualys.com/securitylabs/2015/10/20/clickjacking-a-common-implementation-mistake-that-can-put-your-websites-in-danger.

Detection Information

Parameter	No param has been required for detecting the information.
Authentication	In order to detect this vulnerability, no authentication has been required.
Access Path	Here is the path followed by the scanner to reach the exploitable URL:

https://archibus.vodacom.co.za/archibus/

Payloads

#1 Request

GET https://archibus.vodacom.co.za/favicon.ico

Host: archibus.vodacom.co.za
User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/102.0.5005.177 Safari/537.36
Accept: */*

Click this link to try to reproduce the vulnerability using above payload.Note that clicking this link may not lead to visible results, either because the vulnerability requires context to be previously set (authentication, cookies...) or because the exploitation of the vulnerability does not lead to any visible proof.

#1 Response

The URI was framed.

150263 Insecure Transport (1)

150263 Insecure Transport — *archibus.vodacom.co.za/archibus/* **New**

URL: http://archibus.vodacom.co.za/favicon.ico

Finding #	23859802	**Severity**	Confirmed Vulnerability - Level 3

WAS Web Application Report

Unique #	395fdd08-f864-4a8b-bd78-102257a9f1c0		
Group	Information Disclosure	**First Time Detected**	11 Feb 2024 21:02 GMT+0200
CWE	CWE-319	**Last Time Detected**	11 Feb 2024 21:02 GMT+0200
OWASP	A2 Cryptographic Failures	**Last Time Tested**	11 Feb 2024 21:02 GMT+0200
WASC	WASC-4 INSUFFICIENT TRANSPORT LAYER PROTECTION	**Times Detected**	1

CVSS V3 Base 7.6 **CVSS V3 Temporal** 6.6 **CVSS V3 Attack Vector** Network

Details

Threat

A link is functional over an insecure, HTTP connection. No redirection to HTTPS occurs. Note that this QID is reported for 200/OK responses as well as 4xx and 5xx responses.

Impact

Data sent over a non-HTTPS connection is unencrypted and vulnerable to network sniffing attacks that can expose sensitive or confidential information. This includes non-secure cookies and other potentially sensitive data contained in HTTP headers. Even if no sensitive data is transmitted, man-in-the-middle (MITM) attacks are possible over non-HTTPS connections. An attacker who exploits MITM can intercept and change the conversation between the client (e.g., web browser, mobile device, etc.) and the server.

More information: Why HTTPS Matters

Solution

Ensure that all links are accessible over HTTPS only. The most secure design is for the application to listen and respond only to encrypted HTTPS requests. Alternatively, if non-HTTPS requests are accepted, the server should redirect these requests to HTTPS using a 301 or 302 response.

It is also strongly recommended to use HTTP Strict Transport Security (HSTS) so that web browsers are instructed to use only HTTPS when making requests to the server. QID 150135 will be reported when links without HSTS are found.

For more information, see the Application section of OWASP's Transport Layer Protection Cheat Sheet.

Detection Information

Parameter	No param has been required for detecting the information.
Authentication	In order to detect this vulnerability, no authentication has been required.

Payloads

WAS Web Application Report

#1 Request

GET http://archibus.vodacom.co.za/favicon.ico

Referer: https://archibus.vodacom.co.za/archibus/
Cookie: visid_incap_2776849=2mCPlvHbTaSKgOs2WBZQC/YZyWUAAAAAQUIPAAAAAAAWwMvjPe13zMYdphiXlTQy; nlbi_2776849=ogi1WuqyhRkuEuYJZU49BAAAAABLcyLrdKjEmQdibbXYNFmh; incap_ses_1687_2776849=9uxXXci+jlSe7PgfvG1pF/YZyWUAAAAAfr+BmEPjvWAiYHFjqA+aDQ==;
Host: archibus.vodacom.co.za
User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/102.0.5005.177 Safari/537.36
Accept: */*

Click this link to try to reproduce the vulnerability using above payload.Note that clicking this link may not lead to visible results, either because the vulnerability requires context to be previously set (authentication, cookies...) or because the exploitation of the vulnerability does not lead to any visible proof.

#1 Response

HTTP/1.0 200 OK
Etag: W/"21630-1648737254000"
Last-Modified: Thu, 31 Mar 2022 14:34:14 GMT
Content-Type: image/x-icon
Content-Length: 21630
Cache-Control: max-age=86376, public
Expires: Mon, 12 Feb 2024 19:03:18 GMT
Date: Sun, 11 Feb 2024 19:03:42 GMT
X-CDN: Imperva
Content-Security-Policy-Report-Only: default-src 'self' 'unsafe-eval' 'unsafe-hashes' 'unsafe-inline' data: blob: ; form-action 'none' data: blob: ; report-uri /csp_report
X-Iinfo: 62-26460110-0 0CNN RT(1707678222777 0) q(0 -1 -1 -1) r(0 -1)

150628 Apache Tomcat JsonErrorReportValve Injection Vulnerability (CVE-2022-45143) (1)

150628 Apache Tomcat JsonErrorReportValve Injection Vulnerability (CVE-2022-45143)

archibus.vodacom.co.za/archibus/ **New**

URL: https://archibus.vodacom.co.za/jdl90y5X.1tmhl

Finding #	23859788	**Severity**	Potential Vulnerability - Level 3
Unique #	7ee29436-9e91-400d-b2ba-d5f6dd095fa7		
Group	Information Disclosure	**First Time Detected**	11 Feb 2024 21:02 GMT+0200
CWE	CWE-74	**Last Time Detected**	11 Feb 2024 21:02 GMT+0200
OWASP	A3 Injection	**Last Time Tested**	11 Feb 2024 21:02 GMT+0200
WASC	WASC-13 INFORMATION LEAKAGE	**Times Detected**	1

CVSS V3 Base	7.5	**CVSS V3 Temporal**	6.5	**CVSS V3 Attack Vector**	Network

Details

Threat

Apache Tomcat is an open source web server and servlet container developed by the Apache Software Foundation.

The JsonErrorReportValve did not escape the type, message or description values. In some circumstances these are constructed from user provided data and it was therefore possible for users to supply values that invalidated or manipulated the JSON output.

Affected Versions:
Apache Tomcat 10.1.0-M1 to 10.1.1
Apache Tomcat 9.0.40 to 9.0.68
Apache Tomcat 8.5.83

QID Detection Logic (Unauthenticated):
This QID sends a HTTP GET request to a invalid URL and based on the response confirms the vulnerable instance of Apache Tomcat running on the host.

Impact

Successful exploitation of this vulnerability allows an attacker to supply values that invalidated or manipulated the JSON output.

Solution

Customers are advised to upgrade Apache Tomcat to new version to remediate this vulnerability. For more information please refer to Apache Tomcat Security Advisory.

Detection Information

Parameter	No param has been required for detecting the information.
Authentication	In order to detect this vulnerability, no authentication has been required.

Payloads

#1 Request

GET https://archibus.vodacom.co.za/jdl90y5X.1tmhl

Referer: https://archibus.vodacom.co.za/archibus/
Cookie: visid_incap_2776849=3EQgVogKTdm4B7iU4PcYlZIryWUAAAAAQUIPAAAAAAC13Wpsk2q84RzHqKaSAtCt;
incap_ses_1687_2776849=GVb7ZygGCWNf0xIgvG1pF5IryWUAAAAAC+zeOpT2SLtN/dZ9qy3IyQ==;
Host: archibus.vodacom.co.za
User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/102.0.5005.177 Safari/537.36
Accept: */*

Click this link to try to reproduce the vulnerability using above payload.Note that clicking this link may not lead to visible results, either because the vulnerability requires context to be previously set (authentication, cookies...) or because the exploitation of the vulnerability does not lead to any visible proof.

#1 Response

comment: Apache Tomcat JsonErrorReportValve Injection Vulnerability (CVE-2022-45143) found at PORT : 443

he requested resource [/jdl90y5X.1tmhl] is not available Description The origin server did not find a current representation for the target resource or is not willing to disclose that one exists. <hr class="line" /><h3>Apache Tomcat/9.0.62</h3><script type="text/javascript" src="/_Incapsula_Resource?SWJIYLWA=719d34d31c8e3a6e6fffd425f7e032f3&ns=1&cb=1887381356" async></script></body></html>

* The reflected string on the response webpage indicates that the vulnerability test was successful

150662 Apache Tomcat Information Disclosure Vulnerability (CVE-2023-28708) (1)

150662 Apache Tomcat Information Disclosure Vulnerability (CVE-2023-28708)

archibus.vodacom.co.za/archibus/ **New**

URL: https://archibus.vodacom.co.za/NakF9jB9.1tmhl

Finding #	23859786	**Severity**	Potential Vulnerability - Level 3
Unique #	643092a4-0421-4144-ae11-fdb954f924d6		
Group	Information Disclosure	**First Time Detected**	11 Feb 2024 21:02 GMT+0200
CWE	CWE-523	**Last Time Detected**	11 Feb 2024 21:02 GMT+0200
OWASP	A8 Software and Data Integrity Failures	**Last Time Tested**	11 Feb 2024 21:02 GMT+0200
WASC	WASC-13 INFORMATION LEAKAGE	**Times Detected**	1

CVSS V3 Base	4.3	**CVSS V3 Temporal**	3.8	**CVSS V3 Attack Vector**	Network

Details

Threat

Apache Tomcat is an open source web server and servlet container developed by the Apache Software Foundation.

Tomcat's RemoteIpFilter, when used with HTTP requests received from a reverse proxy that includes the X-Forwarded-Proto header set to https, may cause session cookies created by Tomcat to be transmitted over an insecure channel if the secure attribute is not included in the cookies. This could potentially expose sensitive user data to attackers.

Affected Versions:
Apache Tomcat 11.0.0-M1 to 11.0.0-M2
Apache Tomcat 10.1.0-M1 to 10.1.5
Apache Tomcat 9.0.0-M1 to 9.0.71
Apache Tomcat 8.5.0 to 8.5.85

QID Detection Logic (Unauthenticated):
This QID sends a HTTP GET request to a invalid URL and based on the response confirms the vulnerable instance of Apache Tomcat running on the host.

Impact
Insecure transmission of session cookies could potentially expose sensitive user data to attackers.

Solution
To address this vulnerability, it is recommended that customers upgrade to one of the following versions of Apache Tomcat: 11.0.0-M3, 10.1.6, 9.0.72, or 8.5.86, or install a newer version. For additional information, please refer to the Apache Tomcat Security Advisory.

Detection Information

Parameter	No param has been required for detecting the information.
Authentication	In order to detect this vulnerability, no authentication has been required.

Payloads

#1 Request

GET https://archibus.vodacom.co.za/NakF9jB9.1tmhl
Referer: https://archibus.vodacom.co.za/archibus/
Cookie: visid_incap_2776849=g6jRI+LcT+GE6AgBxajiqcUryWUAAAAAQUIPAAAAAAAaXY3/Y0TiQjybr6ekVsN4; incap_ses_1687_2776849=RqFaJ/84OmYHHxMgvG1pF8UryWUAAAAAXh4AuCM5CHkOAzP2xH80Fg==;
Host: archibus.vodacom.co.za
User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/102.0.5005.177 Safari/537.36
Accept: */*

Click this link to try to reproduce the vulnerability using above payload.Note that clicking this link may not lead to visible results, either because the vulnerability requires context to be previously set (authentication, cookies...) or because the exploitation of the vulnerability does not lead to any visible proof.

#1 Response

comment: Apache Tomcat Information Disclosure Vulnerability (CVE-2023-28708) found at PORT : 443

he requested resource [/NakF9jB9.1tmhl] is not available Description The origin server did not find a current representation for the target resource or is not willing to disclose that one exists. <hr class="line" /><h3>Apache Tomcat/9.0.62</h3><script type="text/javascript" src="/_Incapsula_Resource?SWJIYLWA=719d34d31c8e3a6e6fffd425f7e032f3&ns=1&cb=1967796564" async></script></body></html>

* The reflected string on the response webpage indicates that the vulnerability test was successful

150687 Apache Tomcat FileUpload Denial Of Service (DoS) Vulnerability (CVE-2023-24998) (1)

150687 Apache Tomcat FileUpload Denial Of Service (DoS) Vulnerability (CVE-2023-24998)

archibus.vodacom.co.za/archibus/ **New**

URL: https://archibus.vodacom.co.za/V5I29VIs.1tmhl

Finding #	23859784	**Severity**	Potential Vulnerability - Level 3
Unique #	ffa9a9f6-f845-4e45-b9a5-831f65fb36f9		
Group	Information Disclosure	**First Time Detected**	11 Feb 2024 21:02 GMT+0200
CWE	CWE-770	**Last Time Detected**	11 Feb 2024 21:02 GMT+0200
OWASP	A6 Vulnerable and Outdated Components	**Last Time Tested**	11 Feb 2024 21:02 GMT+0200
WASC		**Times Detected**	

	WASC-10 DENIAL OF SERVICE				1
CVSS V3 Base	7.5	CVSS V3 Temporal	6.7	CVSS V3 Attack Vector	Network

Details

Threat

Apache Tomcat is an open source web server and servlet container developed by the Apache Software Foundation.

Apache Tomcat uses a packaged renamed copy of Apache Commons FileUpload to provide the file upload functionality defined in the Jakarta Servlet specification. Apache Tomcat was, therefore, also vulnerable to the Apache Commons FileUpload vulnerability CVE-2023-24998 as there was no limit to the number of request parts processed. This resulted in the possibility of an attacker triggering a DoS with a malicious upload or series of uploads.

Affected Products:
Apache Tomcat from version 8.5.0 to 8.5.84
Apache Tomcat from version 9.0.0-M1 to 9.0.70
Apache Tomcat from version 10.1.0-M1 to 10.1.4
Apache Tomcat version 11.0.0-M1

QID Detection Logic (Unauthenticated):
This QID sends a HTTP GET request to a invalid URL and based on the response confirms the vulnerable instance of Apache Tomcat running on the host.

Impact

Successful exploitation of the vulnerability can allow an attacker to trigger a DoS via malicious upload or series of uploads

Solution

Upgrade to the Apache Tomcat to the latest version of Apache Tomcat. Please refer to Apache Tomcat 8 Security, Apache Tomcat 9 Security, Apache Tomcat 10 Security, Apache Tomcat 11 Security.

Detection Information

Parameter	No param has been required for detecting the information.
Authentication	In order to detect this vulnerability, no authentication has been required.

Payloads

WAS Web Application Report

#1 Request

GET https://archibus.vodacom.co.za/V5I29VIs.1tmhl

Referer: https://archibus.vodacom.co.za/archibus/
Cookie: visid_incap_2776849=YdS+s3zgSVi/2By94QvPHucryWUAAAAAQUIPAAAAAAAe0lfKbO468RC7TFIV/w1y; incap_ses_1687_2776849=+r43KSN8BV78WRMgvG1pF+cryWUAAAAAofccFu1gONErVRHki8rDoQ==;
Host: archibus.vodacom.co.za
User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/102.0.5005.177 Safari/537.36
Accept: */*

Click this link to try to reproduce the vulnerability using above payload.Note that clicking this link may not lead to visible results, either because the vulnerability requires context to be previously set (authentication, cookies...) or because the exploitation of the vulnerability does not lead to any visible proof.

#1 Response

comment: Apache Tomcat FileUpload Denial Of Service (DoS) Vulnerability (CVE-2023-24998) found at PORT: 443

he requested resource [/V5I29VIs.1tmhl] is not available Description The origin server did not find a current representation for the target resource or is not willing to disclose that one exists. <hr class="line" /><h3>Apache Tomcat/9.0.62</h3><script type="text/javascript" src="/_Incapsula_Resource?SWJIYLWA=719d34d31c8e3a6e6fffd425f7e032f3&ns=1&cb=306739567" async></script></body></html>

* The reflected string on the response webpage indicates that the vulnerability test was successful

150704 Apache Tomcat Open Redirect Vulnerability (CVE-2023-41080) (1)

150704 Apache Tomcat Open Redirect Vulnerability (CVE-2023-41080)

archibus.vodacom.co.za/archibus/ **New**

URL: https://archibus.vodacom.co.za/pIoYCDq1.1tmhl

Finding #	23859782	**Severity**	Potential Vulnerability - Level 3
Unique #	a3215478-4fed-46e4-aadf-82a379e17fb5		
Group	Information Disclosure	**First Time Detected**	11 Feb 2024 21:02 GMT+0200
CWE	CWE-601	**Last Time Detected**	11 Feb 2024 21:02 GMT+0200
OWASP	A3 Injection	**Last Time Tested**	11 Feb 2024 21:02 GMT+0200
WASC	WASC-38 URL REDIRECTOR ABUSE	**Times Detected**	1

CVSS V3 Base	6.1	**CVSS V3 Temporal**	5.3	**CVSS V3 Attack Vector**	Network

Details

Threat

Apache Tomcat is an open source web server and servlet container developed by the Apache Software Foundation.

If the ROOT (default) web application is configured to use FORM authentication then it is possible that a specially crafted URL could be used to trigger a redirect to an URL of the attackers choice.

Affected Versions:
Apache Tomcat 11.0.0-M1 to 11.0.0-M10
Apache Tomcat 10.1.0-M1 to 10.1.12
Apache Tomcat 9.0.0-M1 to 9.0.79
Apache Tomcat 8.5.0 to 8.5.92

QID Detection Logic (Unauthenticated):
This QID sends a HTTP GET request to a invalid URL and based on the response confirms the vulnerable instance of Apache Tomcat running on the host.

Impact

Successful exploitation could allow attackers to trick a user into visiting a specially crafted link which would redirect them to an arbitrary malicious external URL.

Solution

To address this vulnerability, it is recommended that customers upgrade to one of the following versions of Apache Tomcat: 11.0.0-M11, 10.1.13, 9.0.80, or 8.5.93, or install a newer version. For additional information, please refer to the Apache Tomcat Security Advisory.

Detection Information

Parameter	No param has been required for detecting the information.
Authentication	In order to detect this vulnerability, no authentication has been required.

Payloads

#1 Request

GET https://archibus.vodacom.co.za/pIoYCDq1.1tmhl

Referer: https://archibus.vodacom.co.za/archibus/
Cookie: visid_incap_2776849=/+k929TsQfONYWvs136CGU0syWUAAAAAQUIPAAAAAADoDL4gKBV+1aPyUZi9RYz9;
incap_ses_1687_2776849=e1SMV5iDuHnz9BMgvG1pF00syWUAAAAA1/6DQKVeDpjvEsl9CqNoVw==;
Host: archibus.vodacom.co.za
User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/102.0.5005.177 Safari/537.36
Accept: */*

Click this link to try to reproduce the vulnerability using above payload.Note that clicking this link may not lead to visible results, either because the vulnerability requires context to be previously set (authentication, cookies...) or because the exploitation of the vulnerability does not lead to any visible proof.

#1 Response

comment: Apache Tomcat Open Redirect Vulnerability (CVE-2023-41080) found at PORT : 443

he requested resource [/pIoYCDq1.1tmhl] is not available Description The origin server did not find a current representation for the target resource or is not willing to disclose that one exists. <hr class="line" /><h3>Apache Tomcat/9.0.62</h3><script type="text/javascript" src="/_Incapsula_Resource?SWJIYLWA=719d34d31c8e3a6e6fffd425f7e032f3&ns=1&cb=1394971258" async></script></body></html>

* The reflected string on the response webpage indicates that the vulnerability test was successful

150122 Cookie Does Not Contain The "secure" Attribute (2)

150122 Cookie Does Not Contain The "secure" Attribute

archibus.vodacom.co.za/archibus/ **New**

URL: https://archibus.vodacom.co.za/FPRWin/index.aspx

Finding #	23859798	**Severity**	Confirmed Vulnerability - Level 2
Unique #	60d41bad-84d1-4642-904a-1d6c8527c041		
Group	Information Disclosure	**First Time Detected**	11 Feb 2024 21:02 GMT+0200
CWE	CWE-614	**Last Time Detected**	11 Feb 2024 21:02 GMT+0200
OWASP	A5 Security Misconfiguration	**Last Time Tested**	11 Feb 2024 21:02 GMT+0200
WASC	WASC-4 INSUFFICIENT TRANSPORT LAYER PROTECTION	**Times Detected**	1

CVSS V3 Base	4.3	**CVSS V3 Temporal**	4.1	**CVSS V3 Attack Vector**	Network

Details

Threat

The cookie does not contain the "secure" attribute.

Impact

Cookies with the "secure" attribute are only permitted to be sent via HTTPS. Cookies sent via HTTP expose an unsuspecting user to sniffing attacks that could lead to user impersonation or compromise of the application account.

Solution

If the associated risk of a compromised account is high, apply the "secure" attribute to cookies and force all sensitive requests to be sent via HTTPS.

Detection Information

Cookie Name(s) nlbi_2776849_2147483392

Authentication In order to detect this vulnerability, no authentication has been required.

Access Path Here is the path followed by the scanner to reach the exploitable URL:

https://archibus.vodacom.co.za/archibus/
https://archibus.vodacom.co.za/

Payloads

#1 Request

GET https://archibus.vodacom.co.za/FPRWin/index.aspx

Host: archibus.vodacom.co.za
User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/102.0.5005.177 Safari/537.36
Accept: */*

Click this link to try to reproduce the vulnerability using above payload.Note that clicking this link may not lead to visible results, either because the vulnerability requires context to be previously set (authentication, cookies...) or because the exploitation of the vulnerability does not lead to any visible proof.

#1 Response

nlbi_2776849_2147483392=
HTTP/1.1 200 OK
Content-Security-Policy-Report-Only: default-src 'self' 'unsafe-eval' 'unsafe-hashes' 'unsafe-inline' data: blob: ; form-action 'none' data: blob: ; report-uri /csp_report
Set-Cookie: nlbi_2776849_2147483392=/EOeQP34ryLannHzZU49BAAAAAAfvyrl27QIDk3H2LLamNzD; path=/; Domain=.vodacom.co.za
X-CDN: Imperva
X-Iinfo: 41-7406619-7409172 NNNN CT(8 9 0) RT(1707678317790 275989) q(0 0 0 -1) r(1 1)
access-control-allow-origin: *
cache-control: max-age=60
content-encoding: gzip
content-length: 75714
content-type: text/javascript
date: Sun, 11 Feb 2024 19:09:54 GMT
keep-alive: timeout=60
server: bon
server-timing: bon, total;dur=13.402551

150122 Cookie Does Not Contain The "secure" Attribute

archibus.vodacom.co.za/archibus/ **Active**

URL: https://archibus.vodacom.co.za/archibus/

Finding #	18390822	**Severity**	Confirmed Vulnerability - Level 2
Unique #	69e16d6e-848d-41d8-b820-b4599b4ac9b1		
Group	Information Disclosure	**First Time Detected**	22 Jan 2023 21:27 GMT+0200
CWE	CWE-614	**Last Time Detected**	11 Feb 2024 21:02 GMT+0200
OWASP	A5 Security Misconfiguration	**Last Time Tested**	11 Feb 2024 21:02 GMT+0200
WASC	WASC-4 INSUFFICIENT TRANSPORT LAYER PROTECTION	**Times Detected**	15

CVSS V3 Base 4.3 **CVSS V3 Temporal** 4.1 **CVSS V3 Attack Vector** Network

Details

Threat

The cookie does not contain the "secure" attribute.

Impact

Cookies with the "secure" attribute are only permitted to be sent via HTTPS. Cookies sent via HTTP expose an unsuspecting user to sniffing attacks that could lead to user impersonation or compromise of the application account.

Solution

If the associated risk of a compromised account is high, apply the "secure" attribute to cookies and force all sensitive requests to be sent via HTTPS.

Detection Information

Cookie Name(s)	**visid_incap_2776849, incap_ses_1687_2653607, incap_ses_1687_2776849, nlbi_2653607_2147483392, nlbi_2776849, visid_incap_2653607**
Authentication	In order to detect this vulnerability, no authentication has been required.

Payloads

WAS Web Application Report

#1 Request

GET https://archibus.vodacom.co.za/archibus/

Host: archibus.vodacom.co.za
User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/102.0.5005.177 Safari/537.36
Accept: */*

Click this link to try to reproduce the vulnerability using above payload.Note that clicking this link may not lead to visible results, either because the vulnerability requires context to be previously set (authentication, cookies...) or because the exploitation of the vulnerability does not lead to any visible proof.

#1 Response

visid_incap_2776849=2mCPlvHbTaSKgOs2WBZQC/YZyWUAAAAAQUIPAAAAAAAWwMvjPe13zMYdphiXlTQy; expires=Sun Feb 9 22:21:11 2025; path=/; domain=.vodacom.co.za; max-age=31459901; httponly
Cookies set via JavaScript do not have an associated HTTP response header.

incap_ses_1687_2653607=
H2 403
cache-control: no-cache, no-store
content-length: 944
content-security-policy-report-only: font-src 'self' 'unsafe-eval' 'unsafe-hashes' 'unsafe-inline' data: blob: fonts.gstatic.com; form-action *.vodacom.co.za; default-src 'self' 'unsafe-eval' 'unsafe-hashes' 'unsafe-inline' data: blob:; report-uri /csp_report
content-type: text/html
set-cookie: visid_incap_2653607=5WyHTAoQTwOQASGxHqHFwPYZyWUAAAAAQUIPAAAAAAAv++5Sd7WI0erJwGETz3BS; expires=Sun, 09 Feb 2025 22:21:08 GMT; HttpOnly; path=/; Domain=.sso.vodacom.co.za
incap_ses_1687_2653607=pVjWcBFg02Oo7PgfvG1pF/YZyWUAAAAAI+PNsdwCbDKGdroEybsU0w==; path=/; Domain=.sso.vodacom.co.za
x-iinfo: 42-8775126-0 0NNN RT(1707678198347 4) q(0 -1 -1 -1) r(0 -1) B15(11,2006056,0) U18

incap_ses_1687_2776849=9uxXXci+jlSe7PgfvG1pF/YZyWUAAAAAfr+BmEPjvWAiYHFjqA+aDQ==; path=/; domain=.vodacom.co.za
Cookies set via JavaScript do not have an associated HTTP response header.

nlbi_2653607_2147483392=
H2 200
access-control-allow-origin: *
cache-control: max-age=60
content-encoding: gzip
content-length: 75448
content-security-policy-report-only: font-src 'self' 'unsafe-eval' 'unsafe-hashes' 'unsafe-inline' data: blob: fonts.gstatic.com; form-action *.vodacom.co.za; default-src 'self' 'unsafe-eval' 'unsafe-hashes' 'unsafe-inline' data: blob:; report-uri /csp_report
content-type: text/javascript
date: Sun, 11 Feb 2024 19:03:19 GMT
server: bon
server-timing: bon, total;dur=14.634407
set-cookie: nlbi_2653607_2147483392=ph9bJJxIAXaVCw2VoHFvpQAAAAAk8dnUexHo3DCUpnHVyO/T; path=/; Domain=.sso.vodacom.co.za
x-cdn: Imperva
x-iinfo: 40-8123640-8123643 NNNN CT(8 8 0) RT(1707678198364 2) q(0 0 0 5) r(0 1)

nlbi_2776849=ogi1WuqyhRkuEuYJZU49BAAAAABLcyLrdKjEmQdibbXYNFmh; path=/; domain=.vodacom.co.za
Cookies set via JavaScript do not have an associated HTTP response header.

visid_incap_2653607=
H2 403
cache-control: no-cache, no-store
content-length: 944
content-security-policy-report-only: font-src 'self' 'unsafe-eval' 'unsafe-hashes' 'unsafe-inline' data: blob: fonts.gstatic.com; form-action *.vodacom.co.za; default-src 'self' 'unsafe-eval' 'unsafe-hashes' 'unsafe-inline' data: blob:; report-uri /csp_report
content-type: text/html
set-cookie: visid_incap_2653607=5WyHTAoQTwOQASGxHqHFwPYZyWUAAAAAQUIPAAAAAAAv++5Sd7WI0erJwGETz3BS; expires=Sun, 09 Feb 2025 22:21:08 GMT; HttpOnly; path=/; Domain=.sso.vodacom.co.za
incap_ses_1687_2653607=pVjWcBFg02Oo7PgfvG1pF/YZyWUAAAAAI+PNsdwCbDKGdroEybsU0w==; path=/; Domain=.sso.vodacom.co.za
x-iinfo: 42-8775126-0 0NNN RT(1707678198347 4) q(0 -1 -1 -1) r(0 -1) B15(11,2006056,0) U18

150123 Cookie Does Not Contain The "HTTPOnly" Attribute (2)

150123 Cookie Does Not Contain The "HTTPOnly" Attribute

archibus.vodacom.co.za/archibus/ **New**

URL: https://archibus.vodacom.co.za/FPRWin/index.aspx

Finding #	23859796	**Severity**	Confirmed Vulnerability - Level 2
Unique #	3c55da37-ca93-4156-8161-5d43f6193a2a		
Group	Information Disclosure	**First Time Detected**	11 Feb 2024 21:02 GMT+0200
CWE	CWE-1004	**Last Time Detected**	11 Feb 2024 21:02 GMT+0200
OWASP	A5 Security Misconfiguration	**Last Time Tested**	11 Feb 2024 21:02 GMT+0200
WASC	WASC-4 INSUFFICIENT TRANSPORT LAYER PROTECTION	**Times Detected**	1

WAS Web Application Report

CVSS V3 Base	4.3	**CVSS V3 Temporal**	4.1	**CVSS V3 Attack Vector**	Network

Details

Threat
The cookie does not contain the "HTTPOnly" attribute.

Impact
Cookies without the "HTTPOnly" attribute are permitted to be accessed via JavaScript. Cross-site scripting attacks can steal cookies which could lead to user impersonation or compromise of the application account.

Solution
If the associated risk of a compromised account is high, apply the "HTTPOnly" attribute to cookies.

Detection Information

Cookie Name(s)	**nlbi_2776849_2147483392**
Authentication	In order to detect this vulnerability, no authentication has been required.
Access Path	Here is the path followed by the scanner to reach the exploitable URL:

https://archibus.vodacom.co.za/archibus/
https://archibus.vodacom.co.za/

Payloads

#1 Request

GET https://archibus.vodacom.co.za/FPRWin/index.aspx

Host: archibus.vodacom.co.za
User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/102.0.5005.177 Safari/537.36
Accept: */*

Click this link to try to reproduce the vulnerability using above payload.Note that clicking this link may not lead to visible results, either because the vulnerability requires context to be previously set (authentication, cookies...) or because the exploitation of the vulnerability does not lead to any visible proof.

#1 Response

nlbi_2776849_2147483392=
HTTP/1.1 200 OK
Content-Security-Policy-Report-Only: default-src 'self' 'unsafe-eval' 'unsafe-hashes' 'unsafe-inline' data: blob: ; form-action 'none' data: blob: ; report-uri /csp_report
Set-Cookie: nlbi_2776849_2147483392=/EOeQP34ryLannHzZU49BAAAAAAfvyrl27QIDk3H2LLamNzD; path=/; Domain=.vodacom.co.za
X-CDN: Imperva
X-Iinfo: 41-7406619-7409172 NNNN CT(8 9 0) RT(1707678317790 275989) q(0 0 0 -1) r(1 1)
access-control-allow-origin: *
cache-control: max-age=60
content-encoding: gzip
content-length: 75714
content-type: text/javascript
date: Sun, 11 Feb 2024 19:09:54 GMT
keep-alive: timeout=60
server: bon
server-timing: bon, total;dur=13.402551

150123 Cookie Does Not Contain The "HTTPOnly" Attribute

archibus.vodacom.co.za/archibus/ **Active**

URL: https://archibus.vodacom.co.za/archibus/

Finding #	18390824	**Severity**	Confirmed Vulnerability - Level 2
Unique #	31a323a3-00b7-45d6-96d0-369961009647		
Group	Information Disclosure	**First Time Detected**	22 Jan 2023 21:27 GMT+0200

WAS Web Application Report

CWE	CWE-1004	**Last Time Detected**	11 Feb 2024 21:02 GMT+0200
OWASP	A5 Security Misconfiguration	**Last Time Tested**	11 Feb 2024 21:02 GMT+0200
WASC	WASC-4 INSUFFICIENT TRANSPORT LAYER PROTECTION	**Times Detected**	15

CVSS V3 Base	4.3	**CVSS V3 Temporal**	4.1	**CVSS V3 Attack Vector**	Network

Details

Threat
The cookie does not contain the "HTTPOnly" attribute.

Impact
Cookies without the "HTTPOnly" attribute are permitted to be accessed via JavaScript. Cross-site scripting attacks can steal cookies which could lead to user impersonation or compromise of the application account.

Solution
If the associated risk of a compromised account is high, apply the "HTTPOnly" attribute to cookies.

Detection Information

Cookie Name(s)	**nlbi_2776849, incap_ses_1687_2653607, incap_ses_1687_2776849, nlbi_2653607_2147483392**
Authentication	In order to detect this vulnerability, no authentication has been required.

Payloads

#1 Request

GET https://archibus.vodacom.co.za/archibus/

Host: archibus.vodacom.co.za
User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/102.0.5005.177 Safari/537.36
Accept: */*

Click this link to try to reproduce the vulnerability using above payload.Note that clicking this link may not lead to visible results, either because the vulnerability requires context to be previously set (authentication, cookies...) or because the exploitation of the vulnerability does not lead to any visible proof.

#1 Response

nlbi_2776849=ogi1WuqyhRkuEuYJZU49BAAAAABLcyLrdKjEmQdibbXYNFmh; path=/; domain=.vodacom.co.za
Cookies set via JavaScript do not have an associated HTTP response header.

incap_ses_1687_2653607=
H2 403
cache-control: no-cache, no-store
content-length: 944
content-security-policy-report-only: font-src 'self' 'unsafe-eval' 'unsafe-hashes' 'unsafe-inline' data: blob: fonts.gstatic.com; form-action *.vodacom.co.za; default-src 'self' 'unsafe-eval' 'unsafe-hashes' 'unsafe-inline' data: blob:; report-uri /csp_report
content-type: text/html
set-cookie: visid_incap_2653607=5WyHTAoQTwOQASGxHqHFwPYZyWUAAAAAQUIPAAAAAAAv++5Sd7WI0erJwGETz3BS; expires=Sun, 09 Feb 2025 22:21:08 GMT; HttpOnly; path=/; Domain=.sso.vodacom.co.za
incap_ses_1687_2653607=pVjWcBFg02Oo7PgfvG1pF/YZyWUAAAAAI+PNsdwCbDKGdroEybsU0w==; path=/; Domain=.sso.vodacom.co.za
x-iinfo: 42-8775126-0 0NNN RT(1707678198347 4) q(0 -1 -1 -1) r(0 -1) B15(11,2006056,0) U18

incap_ses_1687_2776849=9uxXXci+jlSe7PgfvG1pF/YZyWUAAAAAfr+BmEPjvWAiYHFjqA+aDQ==; path=/; domain=.vodacom.co.za
Cookies set via JavaScript do not have an associated HTTP response header.

nlbi_2653607_2147483392=
H2 200
access-control-allow-origin: *
cache-control: max-age=60
content-encoding: gzip
content-length: 75448
content-security-policy-report-only: font-src 'self' 'unsafe-eval' 'unsafe-hashes' 'unsafe-inline' data: blob: fonts.gstatic.com; form-action *.vodacom.co.za; default-src 'self' 'unsafe-eval' 'unsafe-hashes' 'unsafe-inline' data: blob:; report-uri /csp_report
content-type: text/javascript
date: Sun, 11 Feb 2024 19:03:19 GMT
server: bon
server-timing: bon, total;dur=14.634407
set-cookie: nlbi_2653607_2147483392=ph9bJJxIAXaVCw2VoHFvpQAAAAAk8dnUexHo3DCUpnHVyO/T; path=/; Domain=.sso.vodacom.co.za
x-cdn: Imperva
x-iinfo: 40-8123640-8123643 NNNN CT(8 8 0) RT(1707678198364 2) q(0 0 0 5) r(0 1)

150476 Cookies Issued Without User Consent (1)

150476 Cookies Issued Without User Consent — *archibus.vodacom.co.za/archibus/* **Active**

URL: https://archibus.vodacom.co.za/archibus/

Finding #	18390820	**Severity**	Confirmed Vulnerability - Level 2
Unique #	e3f7b002-7daf-4ad3-9d79-71012ca3984a		
Group	Information Disclosure	**First Time Detected**	22 Jan 2023 21:27 GMT+0200
CWE	CWE-565	**Last Time Detected**	11 Feb 2024 21:02 GMT+0200
OWASP	A5 Security Misconfiguration	**Last Time Tested**	11 Feb 2024 21:02 GMT+0200
WASC	-	**Times Detected**	15

CVSS V3 Base 5.3 **CVSS V3 Temporal** 4.5 **CVSS V3 Attack Vector** Network

Details

Threat
The cookies listed in the Results section were issued from the web application during the crawl without accepting any opt-in dialogs.

Impact
Cookies may be set without user explicitly agreeing to accept them.

Solution

WAS Web Application Report

Review the application to ensure that all cookies listed are supposed to be issued without user opt-in. If the EU Cookie law is applicable for this web application, ensure these cookies require user opt-in or have been classified as exempt by your organization.

Detection Information

Parameter	No param has been required for detecting the information.
Authentication	In order to detect this vulnerability, no authentication has been required.

Payloads

#1 Request

GET https://archibus.vodacom.co.za/archibus/

Host: archibus.vodacom.co.za
User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/102.0.5005.177 Safari/537.36
Accept: */*

Click this link to try to reproduce the vulnerability using above payload.Note that clicking this link may not lead to visible results, either because the vulnerability requires context to be previously set (authentication, cookies...) or because the exploitation of the vulnerability does not lead to any visible proof.

#1 Response

Total cookies: 3
visid_incap_2776849=yVe7wK00QKa1hPO8b86MU5AqyWUAAAAAQUIPAAAAAAA8wMd4LJHdHZcsGFDTrPa1; HttpOnly; expires=Sun, 09-Feb-2025 22:21:08 GMT; domain=.vodacom.co.za; path=/ First set at URL: https://archibus.vodacom.co.za/_Incapsula_Resource?CWUDNSAI=23&xinfo=9-67061412-0 0NNN RT%281681066852139 7%29 q%280 -1 -1 -1%29 r%280 -1%29 B15%284%2C200%2C0%29 U18&incident_id=766000980317811993-326349297580644489&edet=15&cinfo=04000000&rpinfo=0&mth=GET
incap_ses_1687_2776849=5vYiFd3iugQpRREgvG1pF5AqyWUAAAAAOUoZF6NXo8dyuxqCL8eC1Q==; domain=.vodacom.co.za; path=/ First set at URL: https://archibus.vodacom.co.za/_Incapsula_Resource?CWUDNSAI=23&xinfo=9-67061412-0 0NNN RT%281681066852139 7%29 q%280 -1 -1 -1%29 r%280 -1%29 B15%284%2C200%2C0%29 U18&incident_id=766000980317811993-326349297580644489&edet=15&cinfo=04000000&rpinfo=0&mth=GET
nlbi_2776849_2147483392=GpRVW5RLw3kDpdneZU49BAAAAABlFqG3VK0QsDccBNw+7dTO; domain=.vodacom.co.za; path=/ First set at URL: https://archibus.vodacom.co.za/_Incapsula_Resource?CWUDNSAI=23&xinfo=9-67061412-0 0NNN RT%281681066852139 7%29 q%280 -1 -1 -1%29 r%280 -1%29 B15%284%2C200%2C0%29 U18&incident_id=766000980317811993-326349297580644489&edet=15&cinfo=04000000&rpinfo=0&mth=GET

150630 CORS header misconfigured (1)

150630 CORS header misconfigured

archibus.vodacom.co.za/archibus/ **Active**

URL: https://archibus.vodacom.co.za/Leasure-the-deed-will-the-clipt-Angely-ands-Banq?d=archibus.vodacom.co.za

Finding #	19053380	**Severity**	Potential Vulnerability - Level 1
Unique #	c525fc93-6371-4dc8-aac0-1c2bb683dbe1		
Group	Information Disclosure	**First Time Detected**	17 Mar 2023 00:17 GMT+0200
CWE	CWE-942	**Last Time Detected**	11 Feb 2024 21:02 GMT+0200
OWASP	A5 Security Misconfiguration	**Last Time Tested**	11 Feb 2024 21:02 GMT+0200
WASC	-	**Times Detected**	14

CVSS V3 Base	4.3	**CVSS V3 Temporal**	4	**CVSS V3 Attack Vector**	Network

Details

Threat

Cross-Origin Resource Sharing (CORS) is an HTTP-header based mechanism that allows a server to indicate any origins (domain, scheme, or port) other than its own from which a browser should permit loading resources. CORS also relies on a mechanism by which browsers make a "preflight" request to the server hosting the cross-origin resource, in order to check that the server will permit the actual request. In that preflight, the browser sends headers that indicate the HTTP method and headers that will be used in the actual request. For security reasons, browsers restrict cross-origin HTTP requests initiated from scripts. The "Access-Control-Allow-Origin" header is used to specify the allowed origins to access the resource.

The WAS scanning engine detects the vulnerability by examining the "Access-Control-Allow-Origin" header for a wildcard value (*). This value in the response to an XHR request indicate that the resource can be accessed from any domain and needs to be strictly configured.

Impact

If CORS is misconfigured, it can lead to major security risk like access to sensitive data, API keys and other users' data from any domain. This access could lead to misuse and exploitation of protected resource.

Solution

CORS header misconfiguration can be addressed by providing only the list of allowed domains in the "Access-Control-Allow-Origin" header. The wildcard character (*) should never be provided as it indicates any domain can access the resource.

Detection Information

Parameter	No param has been required for detecting the information.
Authentication	In order to detect this vulnerability, no authentication has been required.
Access Path	Here is the path followed by the scanner to reach the exploitable URL:

https://archibus.vodacom.co.za/archibus/
https://archibus.vodacom.co.za/
https://archibus.vodacom.co.za/FPRWin/index.aspx

Payloads

#1 Request

POST https://archibus.vodacom.co.za/Leasure-the-deed-will-the-clipt-Angely-ands-Banq? d=archibus.vodacom.co.za

Origin: http://azbycxdwev.com
Referer: https://archibus.vodacom.co.za/archibus/
Cookie: visid_incap_2776849=2mCPlvHbTaSKgOs2WBZQC/YZyWUAAAAAQUIPAAAAAAAWwMvjPe13zMYdphiXlTQy; nlbi_2776849_2147483392=ceRuWt/xOScjoWiPZU49BAAAAAAAwZFKssMrC5EcTftAT9Ngy; nlbi_2776849=ogi1WuqyhRkuEuYJZU49BAAAAABLcyLrdKjEmQdibbXYNFmh; incap_ses_1687_2776849=9uxXXci+jlSe7PgfvG1pF/YZyWUAAAAAfr+BmEPjvWAiYHFjqA+aDQ==;
Host: archibus.vodacom.co.za
User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/102.0.5005.177 Safari/537.36
Accept: */*
Content-Type: application/x-www-form-urlencoded

-

Click this link to try to reproduce the vulnerability using above payload.Note that clicking this link may not lead to visible results, either because the vulnerability requires context to be previously set (authentication, cookies...) or because the exploitation of the vulnerability does not lead to any visible proof.

#1 Response

comment: CORS header Access-Control-Allow-Origin is misconfigured or is too permissive.

Response headers:
access-control-allow-origin: *
server-timing: bon, total;dur=0.042311999999999995
server: bon
connection: keep-alive
keep-alive: timeout=60
content-length: 0
date: Sun, 11 Feb 2024 19:52:52 GMT
Set-Cookie: nlbi_2776849_2147483392=47ijRzz+MWiouiDMZU49BAAAAACGH86qt3yiA5a4ynJ0pQby; path=/; Domain=.vodacom.co.za
Set-Cookie: incap_ses_1687_2776849=Z971eB99hyoUugcgvG1pF5MlyWUAAAAAF3ud3d+90eSi4ao3G3bclQ==; path=/; Domain=.vodacom.co.za
X-CDN: Imperva
Content-Security-Policy-Report-Only: default-src 'self' 'unsafe-eval' 'unsafe-hashes' 'unsafe-inline' data: blob: ; form-action 'none' data: blob: ; report-uri /csp_report
X-Iinfo: 16-4006792-4006818 NNNN CT(8 8 0) RT(1707681171115 2) q(0 1 1 142) r(1 1) U6

Information Gathered (43)

Information Gathered (1)

150497 Progressive scan completely crawled and tested the website (1)

150497 Progressive scan completely crawled and tested the website

archibus.vodacom.co.za/archibus

Finding #	10974629	**Severity**	Information Gathered - Level 1

Unique #	da2f28d4-647d-4cac-9dcb-963d6666d7d7		
Group	Information Gathered		
CWE	-	**Detection Date**	11 Feb 2024 21:02 GMT+0200
OWASP	-		
WASC	-		

Details

Threat
Scan covered the whole scope of the web application and finished all test phases.
QID is reported, starting from progression 2. When progression 1 is launched and scan is finished it is considered as single scan, hence QID will not be reported. If subsequent scans are completed with all phases QID 150497 will be reported.

Impact
N/A

Solution
Review QID 150021 for additional details of phases completed during this scan.

Results

Scan covered the whole scope of the web application and finished all test phases.

Scan Diagnostics (27)

150018 Connection Error Occurred During Web Application Scan (1)

150018 Connection Error Occurred During Web Application Scan — *archibus.vodacom.co.za/archibus*

Finding #	10541470	**Severity**	Information Gathered - Level 2
Unique #	384bebcf-16d5-489b-a09e-a768ebfafedc		
Group	Scan Diagnostics		
CWE	-	**Detection Date**	11 Feb 2024 21:02 GMT+0200
OWASP	-		
WASC	-		

Details

Threat
The following are some of the possible reasons for the timeouts or connection errors:
1. A disturbance in network connectivity between the scanner and the web application occurred.
2. The web server or application server hosting the application was taken down in the midst of a scan.
3. The web application experienced an overload, possibly due to load generated by the scan.
4. An error occurred in the SSL/TLS handshake (applies to HTTPS web applications only).
5. A security device, such as an IDS/IPS or web application firewall (WAF), began to drop or reject the HTTP connections from the scanner.
6. Very large files like PDFs, videos, etc. are present on the site and caused timeouts when accessed by the scanner.

Impact
Some of the links were not crawled or scanned. Results may be incomplete or incorrect.

Solution
First, confirm that the server was not taken down in the midst of the scan. After that, investigate the root cause by reviewing the listed links and examining web server logs, application server logs, or IDS/IPS/WAF logs. If the errors are caused due to load generated by the scanner then try reducing the scan intensity (this could increase the scan duration). If the errors are due to specific URLs being tested by the scanner or due to specific form data sent by the scanner, then configure exclude lists in the scan configuration as needed to avoid such requests. If timeouts or connection errors are a persistent issue but you want the scan to run to completion, change the Behavior Settings in the option profile to increase the error thresholds or disable the error checks entirely.

WAS Web Application Report

Results

Total number of unique links that encountered timeout errors: 67
Links with highest number of timeouts:
4 https://archibus.vodacom.co.za/
4 https://archibus.vodacom.co.za/docs/config/
3 https://archibus.vodacom.co.za/Leasure-the-deed-will-the-clipt-Angely-ands-Banq?d=archibus.vodacom.co.za
3 https://archibus.vodacom.co.za/archibus/
3 https://archibus.vodacom.co.za/FPRWin/
3 https://archibus.vodacom.co.za/docs/appdev/
2 https://archibus.vodacom.co.za/docs/api/index.html
1 https://archibus.vodacom.co.za/docs/manager-howto.html?wsdl
1 https://archibus.vodacom.co.za/_Incapsula_Resource?SWKMTFSR=1&e=%00%3Cscript%3E_q%3Drandom(X139653882764176Y2_1Z)%3C%2Fscript%3E
1 https://archibus.vodacom.co.za/examples/
1 https://archibus.vodacom.co.za/manager/
1 https://archibus.vodacom.co.za/FPRWin/index.aspxconsole/css/%252e%252e%252fconsole.portal -FORMDATA-_nfpb=true&_pageLabel=&handle=com.bea.core.repackaged.springframework.context.support.FileSystemXmlApplicationContext("http://38bd53a1c45221f6f1a495fbf4813459605b8787.1172143698210219.1304078824.webcgioob15033901.webcgioob.eu2.qualysperiscope.com.")
1 https://archibus.vodacom.co.za/_Incapsula_Resource?CWUDNSAI=23&xinfo=13-50005422-0%200NNN%20RT%2816840910048 23%2015780%29%20q%280%20-1%20-1%201%29%20r%280%20-1%29%20B15%284%2C200%2C0%29%20U18&incident_id=768000330126840138-244105402621364301&edet=15&cinfo=04000000&rpinfo=%22'%3E%3Cqss%20a%3DX27948800Y6_1Z%3E&mth=GET
1 https://archibus.vodacom.co.za/docsconsole/css/%252e%252e%252fconsole.portal -FORMDATA-_nfpb=true&_pageLabel=&handle=com.bea.core.repackaged.springframework.context.support.FileSystemXmlApplicationContext("http://507cba91dc610c277c31e73038572a2f95f9583a.1172143698210219.1634630551.webcgioob15033901.webcgioob.eu2.qualysperiscope.com.")
1 https://archibus.vodacom.co.za/_Incapsula_Resource?CWUDNSAI=23%22xinfo=11-128333115-0%200NNN%20RT%2816865105474 47%202871%29%20q%280%20-1%20-1%200%29%20r%280%20-1%29%20B15%284%2c200%2c0%29%20U18%22incident_id=769000980359807166-612085775202326667%22edet=15%22cinfo=04000000%22rpinfo=0%22mth=GET
1 https://archibus.vodacom.co.za/_Incapsula_Resource?CWUDNSAI=23&xinfo=13-50005422-0%200NNN%20RT%2816840910048 23%2015780%29%20q%280%20-1%20-1%201%29%20r%280%20-1%29%20B15%284%2C200%2C0%29%20U18&incident_id=768000330126840138-244105402621364301&edet=15&cinfo=04000000&rpinfo=0&mth=%22'%3E%3Cqss%20a%3DX27948800Y7_1Z%3E
1 https://archibus.vodacom.co.za/docs/setup.html?wsdl
1 https://archibus.vodacom.co.za/favicon.ico?wsdl
1 https://archibus.vodacom.co.za/manager/status?wsdl
1 https://archibus.vodacom.co.za/docs/security-howto.html
1 https://archibus.vodacom.co.za/_Incapsula_Resource?CWUDNSAI=23%22xinfo=13-50005422-0%200NNN%20RT%2816840910048 23%2015780%29%20q%280%20-1%20-1%201%29%20r%280%20-1%29%20B15%284%2c200%2c0%29%20U18%22incident_id=768000330126840138-244105402621364301%22edet=15%22cinfo=04000000%22rpinfo=0%22mth=GET
1 https://archibus.vodacom.co.za/docs/realm-howto.html
1 https://archibus.vodacom.co.za/manager/html?wsdl
1 https://archibus.vodacom.co.za/_Incapsula_Resource?CWUDNSAI=23&xinfo=13-50005422-0%200NNN%20RT%2816840910048 23%2015780%29%20q%280%20-1%20-1%201%29%20r%280%20-1%29%20B15%284%2C200%2C0%29%20U18&incident_id=%00%3Cscript%3E_q%3Drandom(X27948800Y3_1Z)%3C%2Fscript%3E&edet=15&cinfo=04000000&rpinfo=0&mth=GET
1 https://archibus.vodacom.co.za/host-manager?wsdl
1 https://archibus.vodacom.co.za/_Incapsula_Resource?CWUDNSAI=23&xinfo=%22'%3E%3Cqss%20a%3DX27948800Y2_1Z%3E&incident_id=768000330126840138-244105402621364301&edet=15&cinfo=04000000&rpinfo=0&mth=GET
1 https://archibus.vodacom.co.za/_Incapsula_Resource?CWUDNSAI=23&xinfo=13-50005422-0%200NNN%20RT%2816840910048 23%2015780%29%20q%280%20-1%20-1%201%29%20r%280%20-1%29%20B15%284%2C200%2C0%29%20U18&incident_id=768000330126840138-244105402621364301&edet=15&cinfo=%00%3Cscript%3E_q%3Drandom(X27948800Y5_1Z)%3C%2Fscript%3E&rpinfo=0&mth=GET
1 https://archibus.vodacom.co.za/host-manager/
1 https://archibus.vodacom.co.za/_Incapsula_Resource?SWKMTFSR='%20onEvent%3DX139653882764176Y1_1Z%20&e=0.3450785737536535
1 https://archibus.vodacom.co.za/manager/statusconsole/css/%252e%252e%252fconsole.portal -FORMDATA-_nfpb=true&_pageLabel=&handle=com.bea.core.repackaged.springframework.context.support.FileSystemXmlApplicationContext("http://1378a6de0dcfe4264d8a55525fce8f1533c3925f.1172143698210219.2795546047.webcgioob15033901.webcgioob.eu2.qualysperiscope.com.")
1 https://archibus.vodacom.co.za/_Incapsula_Resource?CWUDNSAI=%22'%3E%3Cqss%20a%3DX27948800Y1_1Z%3E&xinfo=13-50005422-0%200NNN%20RT%2816840910048 23%2015780%29%20q%280%20-1%20-1%201%29%20r%280%20-1%29%20B15%284%2C200%2C0%29%20U18&incident_id=768000330126840138-244105402621364301&edet=15&cinfo=04000000&rpinfo=0&mth=GET
1 https://archibus.vodacom.co.za/docs/cluster-howto.htmlconsole/css/%252e%252e%252fconsole.portal -FORMDATA-_nfpb=true&_pageLabel=&handle=com.bea.core.repackaged.springframework.context.support.FileSystemXmlApplicationContext("http://a945a5cac1b9a95f20bb5cd70760f513eb82fe3c.1172143698210219.4226936628.webcgioob15033901.webcgioob.eu2.qualysperiscope.com.")
1 https://archibus.vodacom.co.za/_Incapsula_Resource?CWUDNSAI=23%22xinfo=10-112012598-0%200NNN%20RT%2816919534447 03%2013039%29%20q%280%20-1%20-1%204%29%20r%280%20-1%29%20B15%284%2c200%2c0%29%20U18%22incident_id=128000730324386403-546957586868474442%22edet=15%22cinfo=04000000%22rpinfo=0%22mth=GET
1 https://archibus.vodacom.co.za/_Incapsula_Resource?CWUDNSAI=23&xinfo=13-50005422-0%200NNN%20RT%2816840910048 23%2015780%29%20q%280%20-1%20-1%201%29%20r%280%20-1%29%20B15%284%2C200%2C0%29%20U18&incident_id=768000330126840138-244105402621364301&edet=%22'%3E%3Cqss%20a%3DX27948800Y4_1Z%3E&cinfo=04000000&rpinfo=0&mth=GET
1 https://archibus.vodacom.co.za/docs/
1 https://archibus.vodacom.co.za/console/css/%252e%252e%252fconsole.portal -FORMDATA-_nfpb=true&_pageLabel=&handle=com.bea.core.repackaged.springframework.context.support.FileSystemXmlApplicationContext("http://51dc64388481a58039d1d54be2abc7d9efb8a7f8.1172143698210219.3671393313.webcgioob15033901.webcgioob.eu2.qualysperiscope.com.")
1 https://archibus.vodacom.co.za/_Incapsula_Resource?CWUDNSAI=23&xinfo=13-50005422-0%200NNN%20RT%2816840910048 23%2015780%29%20q%280%20-1%20-1%201%29%20r%280%20-1%29%20B15%284%2C200%2C0%29%20U18&incident_id=768000330126840138-244105402621364301&edet=15&cinfo=04000000&rpinfo=%00%3Cscript%3E_q%3Drandom(X27948800Y6_1Z)%3C%2Fscript%3E&mth=GET
1 https://archibus.vodacom.co.za/_Incapsula_Resource?CWUDNSAI=23%22xinfo=37-6345043-0%200NNN%20RT%2817052589995 33%2016038%29%20q%280%20-1%20-1%200%29%20r%280%20-1%29%20B15%284%2c200%2c0%29%20U18%22incident_id=168800005032208 7314-407389717989953 01%22edet=15%22cinfo=04000000%22rpinfo=0%22mth=GET
1 https://archibus.vodacom.co.za/FPRWinconsole/css/%252e%252e%252fconsole.portal -FORMDATA-_nfpb=true&_pageLabel=&handle=com.bea.core.repackaged.springframework.context.support.FileSystemXmlApplicationContext("http://c3151e4d27fc871a36f4970d5ef677d2f2e808b1.1172143698210219.3594890796.webcgioob15033901.webcgioob.eu2.qualysperiscope.com.")
1 https://archibus.vodacom.co.za/_Incapsula_Resource?SWKMTFSR=1&e='%20onEvent%3DX139653882764176Y2_1Z%20
1 https://archibus.vodacom.co.za/docs/cluster-howto.html?wsdl
1 https://archibus.vodacom.co.za/docs/security-howto.html?wsdl
1 https://archibus.vodacom.co.za/_Incapsula_Resource?CWUDNSAI=23&xinfo=13-50005422-0%200NNN%20RT%2816840910048 23%2015780%29%20q%280%20-1%20-1%201%29%20r%280%20-1%29%20B15%284%2C200%2C0%29%20U18&incident_id=768000330126840138-244105402621364301&edet=15&cinfo=%22'%3E%3Cqss%20a%3DX27948800Y5_1Z%3E&rpinfo=0&mth=GET
1 https://archibus.vodacom.co.za/_Incapsula_Resource?CWUDNSAI=23%22xinfo=11-74601801-0%200NNN%20RT%2816943725160 63%202785%29%20q%280%20-1%20-1%200%29%20r

%280%20-1%29%20B15%284%2c200%2c0%29%20U18%22incident_id=764000410179907764-353379304890698315%22edet=15%22cinfo=04000000%22rpinfo=0%22mth=GET
1 https://archibus.vodacom.co.za/examplesconsole/css/%252e%252e%252fconsole.portal -FORMDATA-
_nfpb=true&_pageLabel=&handle=com.bea.core.repackaged.springframework.context.support.FileSystemXmlApplicationContext("http://9e30a9eda2021c188181c17a6f908350d407035e.1172143698210219.1973549079.webcgioob15033901.webcgioob.eu2.qualysperiscope.com.")
1 https://archibus.vodacom.co.za/docs/manager-howto.htmlconsole/css/%252e%252e%252fconsole.portal -FORMDATA-
_nfpb=true&_pageLabel=&handle=com.bea.core.repackaged.springframework.context.support.FileSystemXmlApplicationContext("http://aba2ad640bdcc8d2775ea743a46c60dbe3c5bc87.1172143698210219.2100502827.webcgioob15033901.webcgioob.eu2.qualysperiscope.com.")
1 https://archibus.vodacom.co.za/docs/api/
1 https://archibus.vodacom.co.za/FPRWin/index.aspx
1 https://archibus.vodacom.co.za/favicon.icoconsole/css/%252e%252e%252fconsole.portal -FORMDATA-
_nfpb=true&_pageLabel=&handle=com.bea.core.repackaged.springframework.context.support.FileSystemXmlApplicationContext("http://90db8cf4eb34d89381217af0d6a09fb632419325.1172143698210219.2195717658.webcgioob15033901.webcgioob.eu2.qualysperiscope.com.")
1 https://archibus.vodacom.co.za/host-manager/html?wsdl
1 https://archibus.vodacom.co.za/_Incapsula_Resource?CWUDNSAI=23&xinfo=13-50005422-0%200NNN%20RT%2816840910048 23%2015780%29%20q%280%20-1%20-1%201%29%20r%280%20-1%29%20B15%284%2C200%2C0%29%20U18&incident_id=768000330126840138-244105402621364301&edet=15&cinfo=04000000&rpinfo=0&mth=%00%3Cscript%3E_q%3Drandom(X27948800Y7_1Z)%3C%2Fscript%3E
1 https://archibus.vodacom.co.za/_Incapsula_Resource?CWUDNSAI=23&xinfo=13-50005422-0%200NNN%20RT%2816840910048 23%2015780%29%20q%280%20-1%20-1%201%29%20r%280%20-1%29%20B15%284%2C200%2C0%29%20U18&incident_id=768000330126840138-244105402621364301&edet=%00%3Cscript%3E_q%3Drandom(X27948800Y4_1Z)%3C%2Fscript%3E&cinfo=04000000&rpinfo=0&mth=GET
1 https://archibus.vodacom.co.za/_Incapsula_Resource?SWKMTFSR=%22'%3E%3Cqss%20a%3DX139653882764176Y1_1Z%3E&e=0.3450785737536535
1 https://archibus.vodacom.co.za/archibusconsole/css/%252e%252e%252fconsole.portal -FORMDATA-
_nfpb=true&_pageLabel=&handle=com.bea.core.repackaged.springframework.context.support.FileSystemXmlApplicationContext("http://998620e1b199cab4235b5cb3f211802c5b732d44.1172143698210219.2493954658.webcgioob15033901.webcgioob.eu2.qualysperiscope.com.")
1 https://archibus.vodacom.co.za/docs/security-howto.htmlconsole/css/%252e%252e%252fconsole.portal -FORMDATA-
_nfpb=true&_pageLabel=&handle=com.bea.core.repackaged.springframework.context.support.FileSystemXmlApplicationContext("http://627593ef90e0cea5c063b71d2e31229fb07eb7fe.1172143698210219.2271053889.webcgioob15033901.webcgioob.eu2.qualysperiscope.com.")
1 https://archibus.vodacom.co.za/manager?wsdl
1 https://archibus.vodacom.co.za/examples?wsdl
1 https://archibus.vodacom.co.za/_Incapsula_Resource?CWUDNSAI=23&xinfo=%00%3Cscript%3E_q%3Drandom(X27948800Y2_1Z)%3C%2Fscript%3E&incident_id=768000330126840138-244105402621364301&edet=15&cinfo=04000000&rpinfo=0&mth=GET
1 https://archibus.vodacom.co.za/archibus/null
1 https://archibus.vodacom.co.za/_Incapsula_Resource?CWUDNSAI=23%22xinfo=12-143394600-0%200NNN%20RT%2816919534109 96%20780%29%20q%280%20-1%20-1%200%29%20r%280%20-1%29%20B15%284%2c200%2c0%29%20U18%22incident_id=128000730324386403-688694393854497356%22edet=15%22cinfo=04000000%22rpinfo=0%22mth=GET
1 https://archibus.vodacom.co.za/_Incapsula_Resource?SWKMTFSR=1&e=%22'%3E%3Cqss%20a%3DX139653882764176Y2_1Z%3E
1 https://archibus.vodacom.co.za/examples.tar.gz
1 https://archibus.vodacom.co.za/_Incapsula_Resource?CWUDNSAI=23%22xinfo=13-133113832-0%200NNN%20RT%2816999815739671%2015870%29%20q%280%20-1%20-1%200%29%20r%280%20-1%29%20B15%284%2c200%2c0%29%20U18%22incident_id=766001190516980779-728228691682663885%22edet=15%22cinfo=04000000%22rpinfo=0%22mth=GET
1 https://archibus.vodacom.co.za/_Incapsula_Resource?CWUDNSAI=23&xinfo=13-50005422-0%200NNN%20RT%2816840910048 23%2015780%29%20q%280%20-1%20-1%201%29%20r%280%20-1%29%20B15%284%2C200%2C0%29%20U18&incident_id=%22'%3E%3Cqss%20a%3DX27948800Y3_1Z%3E&edet=15&cinfo=04000000&rpinfo=0&mth=GET
1 https://archibus.vodacom.co.za/managerconsole/css/%252e%252e%252fconsole.portal -FORMDATA-
_nfpb=true&_pageLabel=&handle=com.bea.core.repackaged.springframework.context.support.FileSystemXmlApplicationContext("http://8d47be6f68e234566594012f54ac88496e549bfd.1172143698210219.1614632135.webcgioob15033901.webcgioob.eu2.qualysperiscope.com.")
1 https://archibus.vodacom.co.za/_Incapsula_Resource?SWKMTFSR=%00%3Cscript%3E_q%3Drandom(X139653882764176Y1_1Z)%3C%2Fscript%3E&e=0.3450785737536535
1 https://archibus.vodacom.co.za/_Incapsula_Resource?CWUDNSAI=%00%3Cscript%3E_q%3Drandom(X27948800Y1_1Z)%3C%2Fscript%3E&xinfo=13-50005422-0%200NNN%20RT%2816840910048 23%2015780%29%20q%280%20-1%20-1%201%29%20r%280%20-1%29%20B15%284%2C200%2C0%29%20U18&incident_id=768000330126840138-244105402621364301&edet=15&cinfo=04000000&rpinfo=0&mth=GET

Total number of unique links that encountered connection errors: 21
Links with highest number of connection errors:
4 https://archibus.vodacom.co.za/docs/security-howto.html
4 https://archibus.vodacom.co.za/docs/deployer-howto.html
3 https://archibus.vodacom.co.za/manager/html
2 https://archibus.vodacom.co.za/docs/appdev/
2 https://archibus.vodacom.co.za/docs/
2 https://archibus.vodacom.co.za/FPRWin/index.aspx
2 https://archibus.vodacom.co.za/docs/api/
1 https://archibus.vodacom.co.za/docs/cluster-howto.html
1 https://archibus.vodacom.co.za/_Incapsula_Resource?CWUDNSAI=23&xinfo=13-50005422-0%200NNN%20RT%2816840910048 23%2015780%29%20q%280%20-1%20-1%201%29%20r%280%20-1%29%20B15%284%2C200%2C0%29%20U18&incident_id=768000330126840138-244105402621364301&edet='%20onEvent%3DX27948800Y4_1Z%20&cinfo=04000000&rpinfo=0&mth=GET
1 https://archibus.vodacom.co.za/docs/changelog.html
1 https://archibus.vodacom.co.za/docs/RELEASE-NOTES.txt
1 https://archibus.vodacom.co.za/manager/
1 https://archibus.vodacom.co.za/docs/realm-howto.html
1 https://archibus.vodacom.co.za/Leasure-the-deed-will-the-clipt-Angely-ands-Banq?d=archibus.vodacom.co.za
1 https://archibus.vodacom.co.za/_Incapsula_Resource?CWUDNSAI=23&xinfo='%20onEvent%3DX27948800Y2_1Z%20&incident_id=768000330126840138-244105402621364301&edet=15&cinfo=04000000&rpinfo=0&mth=GET
1 https://archibus.vodacom.co.za/null
1 https://archibus.vodacom.co.za/docs/jndi-datasource-examples-howto.html
1 https://archibus.vodacom.co.za/_Incapsula_Resource?CWUDNSAI=23&xinfo=13-50005422-0%200NNN%20RT%2816840910048 23%2015780%29%20q%280%20-1%20-1%201%29%20r%280%20-1%29%20B15%284%2C200%2C0%29%20U18&incident_id='%20onEvent%3DX27948800Y3_1Z%20&edet=15&cinfo=04000000&rpinfo=0&mth=GET
1 https://archibus.vodacom.co.za/host-manager/
1 https://archibus.vodacom.co.za/manager/status
1 https://archibus.vodacom.co.za/_Incapsula_Resource?CWUDNSAI='%20onEvent%3DX27948800Y1_1Z%20&xinfo=13-50005422-0%200NNN%20RT%2816840910048 23%2015780%29%20q%280%20-1%20-1%201%29%20r%280%20-1%29%20B15%284%2C200%2C0%29%20U18&incident_id=768000330126840138-244105402621364301&edet=15&cinfo=04000000&rpinfo=0&mth=GET

Phase wise summary of timeout and connection errors encountered:
ePhaseWSEnumeration : 11 0
ePhaseParameterTests : 20 4
ePhaseWebCgiOob : 27 1
ePhaseCookieTests : 17 6
ePhaseHeaderTests : 6 22
ePhasePathTests : 1 0

WAS Web Application Report

150009 Links Crawled (1)

150009 Links Crawled — *archibus.vodacom.co.za/archibus*

Finding #	10510601	**Severity**	Information Gathered - Level 1
Unique #	4d6af2c2-cdc8-4e63-bdf6-ae5db5dbcf61		
Group	Scan Diagnostics		
CWE	-	**Detection Date**	11 Feb 2024 21:02 GMT+0200
OWASP	-		
WASC	-		

Details

Threat

The list of unique links crawled and HTML forms submitted by the scanner appear in the Results section. This list may contain fewer links than the maximum threshold defined.

NOTE: This list also includes:
- All the unique links that are reported in QID 150140 (Redundant links/URL paths crawled and not crawled)
- All the forms reported in QID 150152 (Forms Crawled)
- All the forms in QID 150115 (Authentication Form Found)
- Certain requests from QID 150172 (Requests Crawled)

Impact

N/A

Solution

N/A

Results

Duration of crawl phase (seconds): 1620.00
Number of links: 111
(This number excludes form requests, ajax links (included in QID 150148) and links re-requested during authentication.)

https://archibus.vodacom.co.za/
https://archibus.vodacom.co.za/FPRWin/
https://archibus.vodacom.co.za/FPRWin/index.aspx
https://archibus.vodacom.co.za/_Incapsula_Resource?CWUDNSAI=23%22xinfo=10-107502277-0%200NNN%20RT%281686510550324%2012994%29%20q%280%20-1%20-1%200%29%20r%280%20-1%29%20B15%284%2c200%2c0%29%20U18%22incident_id=769000980359807166-515218109305526410%22edet=15%22cinfo=04000000%22rpinfo=0%22mth=GET
https://archibus.vodacom.co.za/_Incapsula_Resource?CWUDNSAI=23%22xinfo=10-112012598-0%200NNN%20RT%281691953444703%2013039%29%20q%280%20-1%20-1%204%29%20r%280%20-1%29%20B15%284%2c200%2c0%29%20U18%22incident_id=128000730324386403-546957586868474442%22edet=15%22cinfo=04000000%22rpinfo=0%22mth=GET
https://archibus.vodacom.co.za/_Incapsula_Resource?CWUDNSAI=23%22xinfo=11-128333115-0%200NNN%20RT%281686510547447%202871%29%20q%280%20-1%20-1%200%29%20r%280%20-1%29%20B15%284%2C200%2C0%29%20U18%22incident_id=769000980359807166-612085775202326667%22edet=15%22cinfo=04000000%22rpinfo=0%22mth=GET
https://archibus.vodacom.co.za/_Incapsula_Resource?CWUDNSAI=23%22xinfo=11-128333115-0%200NNN%20RT%281686510547447%202871%29%20q%280%20-1%20-1%200%29%20r%280%20-1%29%20B15%284%2c200%2c0%29%20U18%22incident_id=769000980359807166-612085775202326667%22edet=15%22cinfo=04000000%22rpinfo=0%22mth=GET
https://archibus.vodacom.co.za/_Incapsula_Resource?CWUDNSAI=23%22xinfo=11-74601801-0%200NNN%20RT%281694372516063%202785%29%20q%280%20-1%20-1%200%29%20r%280%20-1%29%20B15%284%2C200%2C0%29%20U18%22incident_id=764000410179907764-353379304890698315%22edet=15%22cinfo=04000000%22rpinfo=0%22mth=GET
https://archibus.vodacom.co.za/_Incapsula_Resource?CWUDNSAI=23%22xinfo=11-74601801-0%200NNN%20RT%281694372516063%202785%29%20q%280%20-1%20-1%200%29%20r%280%20-1%29%20B15%284%2c200%2c0%29%20U18%22incident_id=764000410179907764-353379304890698315%22edet=15%22cinfo=04000000%22rpinfo=0%22mth=GET
https://archibus.vodacom.co.za/_Incapsula_Resource?CWUDNSAI=23%22xinfo=12-140568936-0%200NNN%20RT%281699815739671%202292%29%20q%280%20-1%20-1%201%29%20r%280%20-1%29%20B15%284%2c200%2c0%29%20U18%22incident_id=766001190516980779-773471142739320268%22edet=15%22cinfo=04000000%22rpinfo=0%22mth=GET
https://archibus.vodacom.co.za/_Incapsula_Resource?CWUDNSAI=23%22xinfo=12-143394600-0%200NNN%20RT%281691953410996%20780%29%20q%280%20-1%20-1%200%29%20r%280%20-1%29%20B15%284%2c200%2c0%29%20U18%22incident_id=128000730324386403-688694393854497356%22edet=15%22cinfo=04000000%22rpinfo=0%22mth=GET
https://archibus.vodacom.co.za/_Incapsula_Resource?CWUDNSAI=23%22xinfo=13-133113832-0%200NNN%20RT%281699815739671%2015870%29%20q%280%20-1%20-1%200%29%20r%280%20-1%29%20B15%284%2c200%2c0%29%20U18%22incident_id=766001190516980779-7282286916826638 85%22edet=15%22cinfo=04000000%22rpinfo=0%22mth=GET
https://archibus.vodacom.co.za/_Incapsula_Resource?CWUDNSAI=23%22xinfo=13-50005422-0%200NNN%20RT%281684091004823%2015780%29%20q%280%20-1%20-1%201%29%20r%280%20-1%29%20B15%284%2c200%2c0%29%20U18%22incident_id=768000330126840138-244105402621364301%22edet=15%22cinfo=04000000%22rpinfo=0%22mth=GET
https://archibus.vodacom.co.za/_Incapsula_Resource?CWUDNSAI=23%22xinfo=13-51475396-0%200NNN%20RT%281696791744809%202625%29%20q%280%20-1%20-1%202%29%20r%280%20-1%29%20B15%284%2c200%2c0%29%20U18%22incident_id=764000460129603047-261986575540030349%22edet=15%22cinfo=04000000%22rpinfo=0%22mth=GET
https://archibus.vodacom.co.za/_Incapsula_Resource?CWUDNSAI=23%22xinfo=13-51475397-0%200NNN%20RT%281696791744809%2015891%29%20q%280%20-1%20-1%200%29%20r%280%20-1%29%20B15%284%2c200%2c0%29%20U18%22incident_id=764000460129603047-262001204198640525%22edet=15%22cinfo=04000000%22rpinfo=0%22mth=GET
https://archibus.vodacom.co.za/_Incapsula_Resource?CWUDNSAI=23%22xinfo=14-56552041-0%200NNN%20RT%281684091004822%202271%29%20q%280%20-1%20-1%200%29%20r%280%20-1%29%20B15%284%2c200%2c0%29%20U18%22incident_id=768000330126840138-290605261188499534%22edet=15%22cinfo=04000000%22rpinfo=0%22mth=GET
https://archibus.vodacom.co.za/_Incapsula_Resource?CWUDNSAI=23%22xinfo=36-7073891-0%200NNN%20RT%281705258999531%202780%29%20q%280%20-1%20-1%200%29%20r%280%20-1%29%20B15%284%2c200%2c0%29%20U18%22incident_id=168800005032208 7314-449426280902823 40%22edet=15%22cinfo=04000000%22rpinfo=0%22mth=GET

WAS Web Application Report

https://archibus.vodacom.co.za/_Incapsula_Resource?CWUDNSAI=23%22xinfo=37-6345043-0%200NNN%20RT%281705258999533%2016038%29%20q%280%20-1%20-1%200%29%20r
%280%20-1%29%20B15%284%2c200%2c0%29%20U18%22incident_id=16880000503220873 14-4073897179899530 1%22edet=15%22cinfo=04000000%22rpinfo=0%22mth=GET
https://archibus.vodacom.co.za/_Incapsula_Resource?CWUDNSAI=23%22xinfo=4-9346511-0%200NNN%20RT%281694372516064%2015875%29%20q%280%20-1%20-1%200%29%20r
%280%20-1%29%20B15%284%2c200%2c0%29%20U18%22incident_id=7640004101799077 64-4560220615737606 8%22edet=15%22cinfo=04000000%22rpinfo=0%22mth=GET
https://archibus.vodacom.co.za/_Incapsula_Resource?CWUDNSAI=23%22xinfo=5-218372829-0%200NNN%20RT%2816889292454117%202786%29%20q%280%20-1%20-1%201%29%20r
%280%20-1%29%20B15%284%2c200%2c0%29%20U18%22incident_id=44900158057159480 0-1118955442970634117%22edet=15%22cinfo=04000000%22rpinfo=0%22mth=GET
https://archibus.vodacom.co.za/_Incapsula_Resource?CWUDNSAI=23%22xinfo=5-85633350-0%200NNN%20RT%2817022349356 13%208793%29%20q%280%20-1%20-1%200%29%20r
%280%20-1%29%20B15%284%2c200%2c0%29%20U18%22incident_id=7700011704369758 87-4304587722600031 41%22edet=15%22cinfo=04000000%22rpinfo=0%22mth=GET
https://archibus.vodacom.co.za/_Incapsula_Resource?CWUDNSAI=23%22xinfo=6-50761907-0%200NNN%20RT%2816919534291 71%2013568%29%20q%280%20-1%20-1%200%29%20r
%280%20-1%29%20B15%284%2c200%2c0%29%20U18%22incident_id=12800073032438640 3-2572967890386990 78%22edet=15%22cinfo=04000000%22rpinfo=0%22mth=GET
https://archibus.vodacom.co.za/_Incapsula_Resource?CWUDNSAI=23%22xinfo=7-120841302-0%200NNN%20RT%2816889294541 19%2016073%29%20q%280%20-1%20-1%200%29%20r
%280%20-1%29%20B15%284%2c200%2c0%29%20U18%22incident_id=44900158057159480 0-6317380122245303 11%22edet=15%22cinfo=04000000%22rpinfo=0%22mth=GET
https://archibus.vodacom.co.za/_Incapsula_Resource?CWUDNSAI=23%22xinfo=7-74746777-0%200NNN%20RT%2817022349285 35%202882%29%20q%280%20-1%20-1%200%29%20r
%280%20-1%29%20B15%284%2c200%2c0%29%20U18%22incident_id=7700011704369758 87-3762828923068818 63%22edet=15%22cinfo=04000000%22rpinfo=0%22mth=GET
https://archibus.vodacom.co.za/_Incapsula_Resource?CWUDNSAI=23%22xinfo=8-71777546-0%200NNN%20RT%2816919534158 95%209146%29%20q%280%20-1%20-1%202%29%20r
%280%20-1%29%20B15%284%2c200%2c0%29%20U18%22incident_id=12800073032438640 3-3553915559234565 84%22edet=15%22cinfo=04000000%22rpinfo=0%22mth=GET
https://archibus.vodacom.co.za/_Incapsula_Resource?CWUDNSAI=23&xinfo=10-107502277-0%200NNN%20RT%281686510550324%2012994%29%20q%280%20-1%20-1%200%29%20r
%280%20-1%29%20B15%284%2C200%2C0%29%20U18&incident_id=7690009803598071 66-5152181093055264 10&edet=15&cinfo=04000000&rpinfo=0&mth=GET
https://archibus.vodacom.co.za/_Incapsula_Resource?CWUDNSAI=23&xinfo=10-112005025-0%200NNN%20RT%2816919534089 43%2013%29%20q%280%20-1%20-1%29%20r
%280%20-1%29%20B15%284%2C200%2C0%29%20U18&incident_id=1280007303243864 03-5469087659752208 10&edet=15&cinfo=04000000&rpinfo=0&mth=GET
https://archibus.vodacom.co.za/_Incapsula_Resource?CWUDNSAI=23&xinfo=10-112007274-0%200NNN%20RT%2816919534186 47%206%29%20q%280%20-1%20-1%200%29%20r
%280%20-1%29%20B15%284%2c200%2c0%29%20U18&incident_id=1280007303243864 03-5469194089041802 98&edet=15&cinfo=04000000&rpinfo=0&mth=GET
https://archibus.vodacom.co.za/_Incapsula_Resource?CWUDNSAI=23&xinfo=10-64315409-0%200NNN%20RT%2816943725160 43%2013%29%20q%280%20-1%20-1%29%20r
%280%20-1%29%20B15%284%2C200%2C0%29%20U18&incident_id=7640004101799077 64-3092177854332954 34&edet=15&cinfo=04000000&rpinfo=0&mth=GET
https://archibus.vodacom.co.za/_Incapsula_Resource?CWUDNSAI=23&xinfo=11-113096202-0%200NNN%20RT%2816810668557 38%2015577%29%20q%280%20-1%20-1%200%29%20r
%280%20-1%29%20B15%284%2C200%2C0%29%20U18&incident_id=7660009803178119 93-5515624403916617 07&edet=15&cinfo=04000000&rpinfo=0&mth=GET
https://archibus.vodacom.co.za/_Incapsula_Resource?CWUDNSAI=23&xinfo=11-113096202-0%200NNN%20RT%2816810668557 38%2015577%29%20q%280%20-1%20-1%200%29%20r
%280%20-1%29%20B15%284%2c200%2c0%29%20U18&incident_id=7660009803178119 93-5515624403916617 07&edet=15&cinfo=04000000&rpinfo=0&mth=GET
https://archibus.vodacom.co.za/_Incapsula_Resource?CWUDNSAI=23&xinfo=11-128333115-0%200NNN%20RT%2816865105474 47%202871%29%20q%280%20-1%20-1%200%29%20r
%280%20-1%29%20B15%284%2C200%2C0%29%20U18&incident_id=7690009803598071 66-6120857752023266 67&edet=15&cinfo=04000000&rpinfo=0&mth=GET
https://archibus.vodacom.co.za/_Incapsula_Resource?CWUDNSAI=23&xinfo=11-74601801-0%200NNN%20RT%2816943725160 63%202785%29%20q%280%20-1%20-1%200%29%20r
%280%20-1%29%20B15%284%2C200%2C0%29%20U18&incident_id=7640004101799077 64-3533793048906983 15&edet=15&cinfo=04000000&rpinfo=0&mth=GET
https://archibus.vodacom.co.za/_Incapsula_Resource?CWUDNSAI=23&xinfo=12-134233322-0%200NNN%20RT%2816810668557 20%209%29%20q%280%20-1%20-1%20-1%29%20r
%280%20-1%29%20B15%284%2C200%2C0%29%20U18&incident_id=7660009803178119 93-6509865910821254 52&edet=15&cinfo=04000000&rpinfo=0&mth=GET
https://archibus.vodacom.co.za/_Incapsula_Resource?CWUDNSAI=23&xinfo=12-140568936-0%200NNN%20RT%2816998157396 71%202292%29%20q%280%20-1%20-1%201%29%20r
%280%20-1%29%20B15%284%2C200%2C0%29%20U18&incident_id=7660011905169807 79-7734711427393202 68&edet=15&cinfo=04000000&rpinfo=0&mth=GET
https://archibus.vodacom.co.za/_Incapsula_Resource?CWUDNSAI=23&xinfo=12-143394600-0%200NNN%20RT%2816919534109 96%20780%29%20q%280%20-1%20-1%200%29%20r
%280%20-1%29%20B15%284%2C200%2C0%29%20U18&incident_id=1280007303243864 03-6886943938544973 56&edet=15&cinfo=04000000&rpinfo=0&mth=GET
https://archibus.vodacom.co.za/_Incapsula_Resource?CWUDNSAI=23&xinfo=12-44624439-0%200NNN%20RT%2816840910048 03%2012%29%20q%280%20-1%20-1%29%20r
%280%20-1%29%20B15%284%2C200%2C0%29%20U18&incident_id=7680003301268401 38-2309901659322471 66&edet=15&cinfo=04000000&rpinfo=0&mth=GET
https://archibus.vodacom.co.za/_Incapsula_Resource?CWUDNSAI=23&xinfo=12-46623679-0%200NNN%20RT%2816967917447 90%2011%29%20q%280%20-1%20-1%20-1%29%20r
%280%20-1%29%20B15%284%2C200%2C0%29%20U18&incident_id=7640004601296030 47-2386697392559256 44&edet=15&cinfo=04000000&rpinfo=0&mth=GET
https://archibus.vodacom.co.za/_Incapsula_Resource?CWUDNSAI=23&xinfo=12-46625623-0%200NNN%20RT%2816967917543 09%203%29%20q%280%20-1%20-1%201%29%20r
%280%20-1%29%20B15%284%2c200%2c0%29%20U18&incident_id=7640004601296030 47-2386796176807064 44&edet=15&cinfo=04000000&rpinfo=0&mth=GET
https://archibus.vodacom.co.za/_Incapsula_Resource?CWUDNSAI=23&xinfo=13-115516529-0%200NNN%20RT%2817022349377 15%206%29%20q%280%20-1%20-1%200%29%20r
%280%20-1%29%20B15%284%2c200%2c0%29%20U18&incident_id=7700011704369758 87-6108841679070242 05&edet=15&cinfo=04000000&rpinfo=0&mth=GET
https://archibus.vodacom.co.za/_Incapsula_Resource?CWUDNSAI=23&xinfo=13-133113832-0%200NNN%20RT%2816998157396 71%2015870%29%20q%280%20-1%20-1%200%29%20r
%280%20-1%29%20B15%284%2C200%2C0%29%20U18&incident_id=7660011905169807 79-7282286916826638 85&edet=15&cinfo=04000000&rpinfo=0&mth=GET
https://archibus.vodacom.co.za/_Incapsula_Resource?CWUDNSAI=23&xinfo=13-176129679-0%200NNN%20RT%281686510556626%204%29%20q%280%20-1%20-1%200%29%20r
%280%20-1%29%20B15%284%2c200%2c0%29%20U18&incident_id=7690009803598071 66-8338843030489068 93&edet=15&cinfo=04000000&rpinfo=0&mth=GET
https://archibus.vodacom.co.za/_Incapsula_Resource?CWUDNSAI=23&xinfo=13-49979840-0%200NNN%20RT%2816840909002 25%203%29%20q%280%20-1%20-1%20-1%29%20r
%280%20-1%29%20B15%284%2c200%2c0%29%20U18&incident_id=7680003301268401 38-2439719622824448 77&edet=15&cinfo=04000000&rpinfo=0&mth=GET
https://archibus.vodacom.co.za/_Incapsula_Resource?CWUDNSAI=23&xinfo=13-50005422-0%200NNN%20RT%2816840910048 23%2015780%29%20q%280%20-1%20-1%201%29%20r
%280%20-1%29%20B15%284%2C200%2C0%29%20U18&incident_id=7680003301268401 38-2441054026213643 01&edet=15&cinfo=04000000&rpinfo=0&mth=GET
https://archibus.vodacom.co.za/_Incapsula_Resource?CWUDNSAI=23&xinfo=13-51475396-0%200NNN%20RT%2816967917448 09%202625%29%20q%280%20-1%20-1%202%29%20r
%280%20-1%29%20B15%284%2C200%2C0%29%20U18&incident_id=7640004601296030 47-2619865755400303 49&edet=15&cinfo=04000000&rpinfo=0&mth=GET
https://archibus.vodacom.co.za/_Incapsula_Resource?CWUDNSAI=23&xinfo=13-51475397-0%200NNN%20RT%2816967917448 09%2015891%29%20q%280%20-1%20-1%200%29%20r
%280%20-1%29%20B15%284%2C200%2C0%29%20U18&incident_id=7640004601296030 47-2620012041986405 25&edet=15&cinfo=04000000&rpinfo=0&mth=GET
https://archibus.vodacom.co.za/_Incapsula_Resource?CWUDNSAI=23&xinfo=14-126467959-0%200NNN%20RT%2817022349285 13%2014%29%20q%280%20-1%20-1%20-1%29%20r
%280%20-1%29%20B15%284%2C200%2C0%29%20U18&incident_id=7700011704369758 87-6607550947651822 86&edet=15&cinfo=04000000&rpinfo=0&mth=GET
https://archibus.vodacom.co.za/_Incapsula_Resource?CWUDNSAI=23&xinfo=14-178098704-0%200NNN%20RT%281681066855737%202281%29%20q%280%20-1%20-1%208%29%20r
%280%20-1%29%20B15%284%2C200%2C0%29%20U18&incident_id=7660009803178119 93-8627423343394223 50&edet=15&cinfo=04000000&rpinfo=0&mth=GET
https://archibus.vodacom.co.za/_Incapsula_Resource?CWUDNSAI=23&xinfo=14-178098704-0%200NNN%20RT%281681066855737%202281%29%20q%280%20-1%20-1%208%29%20r
%280%20-1%29%20B15%284%2c200%2c0%29%20U18&incident_id=7660009803178119 93-8627423343394223 50&edet=15&cinfo=04000000&rpinfo=0&mth=GET
https://archibus.vodacom.co.za/_Incapsula_Resource?CWUDNSAI=23&xinfo=14-178100241-0%200NNN%20RT%281681066864525%202%29%20q%280%20-1%20-1%200%29%20r
%280%20-1%29%20B15%284%2c200%2c0%29%20U18&incident_id=7660009803178119 93-8627472692568454 54&edet=15&cinfo=04000000&rpinfo=0&mth=GET
https://archibus.vodacom.co.za/_Incapsula_Resource?CWUDNSAI=23&xinfo=14-56552041-0%200NNN%20RT%2816840910048 22%202271%29%20q%280%20-1%20-1%200%29%20r
%280%20-1%29%20B15%284%2C200%2C0%29%20U18&incident_id=7680003301268401 38-2906052611884995 34&edet=15&cinfo=04000000&rpinfo=0&mth=GET
https://archibus.vodacom.co.za/_Incapsula_Resource?CWUDNSAI=23&xinfo=14-99576411-0%200NNN%20RT%2816943725126 06%209%29%20q%280%20-1%20-1%20-1%29%20r
%280%20-1%29%20B15%284%2c200%2c0%29%20U18&incident_id=7640004101799077 64-4646817975236060 94&edet=15&cinfo=04000000&rpinfo=0&mth=GET
https://archibus.vodacom.co.za/_Incapsula_Resource?CWUDNSAI=23&xinfo=14-99580654-0%200NNN%20RT%2816943725251 49%204%29%20q%280%20-1%20-1%200%29%20r
%280%20-1%29%20B15%284%2c200%2c0%29%20U18&incident_id=7640004101799077 64-4647016059127752 46&edet=15&cinfo=04000000&rpinfo=0&mth=GET
https://archibus.vodacom.co.za/_Incapsula_Resource?CWUDNSAI=23&xinfo=16-2346944-0%200NNN%20RT%281705258999514%2010%29%20q%280%20-1%20-1%20-1%29%20r
%280%20-1%29%20B15%284%2c200%2c0%29%20U18&incident_id=1688000050322087 31-1614737204156859 2&edet=15&cinfo=04000000&rpinfo=0&mth=GET
https://archibus.vodacom.co.za/_Incapsula_Resource?CWUDNSAI=23&xinfo=36-7073891-0%200NNN%20RT%281705258999531%202780%29%20q%280%20-1%20-1%200%29%20r
%280%20-1%29%20B15%284%2c200%2c0%29%20U18&incident_id=1688000050322087 14-4494262809028234 0&edet=15&cinfo=04000000&rpinfo=0&mth=GET
https://archibus.vodacom.co.za/_Incapsula_Resource?CWUDNSAI=23&xinfo=37-6345043-0%200NNN%20RT%281705258999533%2016038%29%20q%280%20-1%20-1%200%29%20r
%280%20-1%29%20B15%284%2c200%2c0%29%20U18&incident_id=1688000050322087 31-4073897179899530 1&edet=15&cinfo=04000000&rpinfo=0&mth=GET
https://archibus.vodacom.co.za/_Incapsula_Resource?CWUDNSAI=23&xinfo=4-185001335-0%200NNN%20RT%2816888929350663%207%29%20q%280%20-1%20-1%20-1%29%20r
%280%20-1%29%20B15%284%2c200%2c0%29%20U18&incident_id=4490015805715948 00-9499091938071776 04&edet=15&cinfo=04000000&rpinfo=0&mth=GET
https://archibus.vodacom.co.za/_Incapsula_Resource?CWUDNSAI=23&xinfo=4-6583483-0%200NNN%20RT%2816967916769 41%203%29%20q%280%20-1%20-1%20-1%29%20r
%280%20-1%29%20B15%284%2c200%2c0%29%20U18&incident_id=7640004601296030 47-3405978649205440 4&edet=15&cinfo=04000000&rpinfo=0&mth=GET
https://archibus.vodacom.co.za/_Incapsula_Resource?CWUDNSAI=23&xinfo=4-77155952-0%200NNN%20RT%2816998157487 53%203%29%20q%280%20-1%20-1%200%29%20r
%280%20-1%29%20B15%284%2c200%2c0%29%20U18&incident_id=7660011905169807 79-4342367242775505 32&edet=15&cinfo=04000000&rpinfo=0&mth=GET
https://archibus.vodacom.co.za/_Incapsula_Resource?CWUDNSAI=23&xinfo=4-9346511-0%200NNN%20RT%281694372516064%2015875%29%20q%280%20-1%20-1%200%29%20r

%280%20-1%29%20B15%284%2C200%2C0%29%20U18&incident_id=764000410179907764-456022061573760 68&edet=15&cinfo=04000000&rpinfo=0&mth=GET
https://archibus.vodacom.co.za/_Incapsula_Resource?CWUDNSAI=23&xinfo=5-102401836-0%200NNN%20RT%281686510484694%203%29%20q%280%20-1%20-1%20-1%29%20r
%280%20-1%29%20B15%284%2c200%2c0%29%20U18&incident_id=769000980359807166-486662297683564677&edet=15&cinfo=04000000&rpinfo=0&mth=GET
https://archibus.vodacom.co.za/_Incapsula_Resource?CWUDNSAI=23&xinfo=5-218372829-0%200NNN%20RT%281688929454117%202786%29%20q%280%20-1%20-1%201%29%20r
%280%20-1%29%20B15%284%2C200%2C0%29%20U18&incident_id=449001580571594800-11189554429706341 17&edet=15&cinfo=04000000&rpinfo=0&mth=GET
https://archibus.vodacom.co.za/_Incapsula_Resource?CWUDNSAI=23&xinfo=5-218374445-0%200NNN%20RT%281688929463409%203%29%20q%280%20-1%20-1%200%29%20r
%280%20-1%29%20B15%284%2c200%2c0%29%20U18&incident_id=449001580571594800-11189615289392925 49&edet=15&cinfo=04000000&rpinfo=0&mth=GET
https://archibus.vodacom.co.za/_Incapsula_Resource?CWUDNSAI=23&xinfo=5-85625692-0%200NNN%20RT%2817022348659 69%203%29%20q%280%20-1%20-1%20-1%29%20r
%280%20-1%29%20B15%284%2c200%2c0%29%20U18&incident_id=770011704369758 87-4304178369267049 65&edet=15&cinfo=04000000&rpinfo=0&mth=GET
https://archibus.vodacom.co.za/_Incapsula_Resource?CWUDNSAI=23&xinfo=5-85633350-0%200NNN%20RT%2817022349356 13%208793%29%20q%280%20-1%20-1%200%29%20r
%280%20-1%29%20B15%284%2C200%2C0%29%20U18&incident_id=770011704369758 87-4304587722600031 41&edet=15&cinfo=04000000&rpinfo=0&mth=GET
https://archibus.vodacom.co.za/_Incapsula_Resource?CWUDNSAI=23&xinfo=57-14510035-0%200NNN%20RT%281705258916770%204%29%20q%280%20-1%20-1%20-1%29%20r
%280%20-1%29%20B15%284%2c200%2c0%29%20U18&incident_id=168800005032208731 4-905673312362827 45&edet=15&cinfo=04000000&rpinfo=0&mth=GET
https://archibus.vodacom.co.za/_Incapsula_Resource?CWUDNSAI=23&xinfo=6-50761907-0%200NNN%20RT%2816919534291 71%2013568%29%20q%280%20-1%20-1%200%29%20r
%280%20-1%29%20B15%284%2C200%2C0%29%20U18&incident_id=128000730324386403-257296789038699078&edet=15&cinfo=04000000&rpinfo=0&mth=GET
https://archibus.vodacom.co.za/_Incapsula_Resource?CWUDNSAI=23&xinfo=6-59075188-0%200NNN%20RT%2816999815693202%203%29%20q%280%20-1%20-1%20-1%29%20r
%280%20-1%29%20B15%284%2c200%2c0%29%20U18&incident_id=766001190516980779-333163456469278150&edet=15&cinfo=04000000&rpinfo=0&mth=GET
https://archibus.vodacom.co.za/_Incapsula_Resource?CWUDNSAI=23&xinfo=7-120841300-0%200NNN%20RT%2816888929454097%2014%29%20q%280%20-1%20-1%20-1%29%20r
%280%20-1%29%20B15%284%2C200%2C0%29%20U18&incident_id=449001580571594800-631729216131508103&edet=15&cinfo=04000000&rpinfo=0&mth=GET
https://archibus.vodacom.co.za/_Incapsula_Resource?CWUDNSAI=23&xinfo=7-120841302-0%200NNN%20RT%2816888929454119%2016073%29%20q%280%20-1%20-1%200%29%20r
%280%20-1%29%20B15%284%2C200%2C0%29%20U18&incident_id=449001580571594800-631738012245303 11&edet=15&cinfo=04000000&rpinfo=0&mth=GET
https://archibus.vodacom.co.za/_Incapsula_Resource?CWUDNSAI=23&xinfo=7-2288043-0%200NNN%20RT%281705259009181%203%29%20q%280%20-1%20-1%201%29%20r
%280%20-1%29%20B15%284%2c200%2c0%29%20U18&incident_id=168800005032208731 4-163543035658898 63&edet=15&cinfo=04000000&rpinfo=0&mth=GET
https://archibus.vodacom.co.za/_Incapsula_Resource?CWUDNSAI=23&xinfo=7-74746777-0%200NNN%20RT%2817022349285 35%202882%29%20q%280%20-1%20-1%200%29%20r
%280%20-1%29%20B15%284%2C200%2C0%29%20U18&incident_id=770011704369758 87-3762828923068818 63&edet=15&cinfo=04000000&rpinfo=0&mth=GET
https://archibus.vodacom.co.za/_Incapsula_Resource?CWUDNSAI=23&xinfo=8-71777546-0%200NNN%20RT%2816919534158 95%209146%29%20q%280%20-1%20-1%202%29%20r
%280%20-1%29%20B15%284%2C200%2C0%29%20U18&incident_id=128000730324386403-355359155923456584&edet=15&cinfo=04000000&rpinfo=0&mth=GET
https://archibus.vodacom.co.za/_Incapsula_Resource?CWUDNSAI=23&xinfo=9-31678237-0%200NNN%20RT%2816840910138 78%203%29%20q%280%20-1%20-1%201%29%20r
%280%20-1%29%20B15%284%2c200%2c0%29%20U18&incident_id=768000330126840138-156191708449605705&edet=15&cinfo=04000000&rpinfo=0&mth=GET
https://archibus.vodacom.co.za/_Incapsula_Resource?CWUDNSAI=23&xinfo=9-67061412-0%200NNN%20RT%2816810668521 39%207%29%20q%280%20-1%20-1%20-1%29%20r
%280%20-1%29%20B15%284%2c200%2c0%29%20U18&incident_id=766000980317811993-326349297580644489&edet=15&cinfo=04000000&rpinfo=0&mth=GET
https://archibus.vodacom.co.za/_Incapsula_Resource?CWUDNSAI=23&xinfo=9-82952600-0%200NNN%20RT%2816865105474 26%2013%29%20q%280%20-1%20-1%20-1%29%20r
%280%20-1%29%20B15%284%2C200%2C0%29%20U18&incident_id=769000980359807166-403616321876596873&edet=15&cinfo=04000000&rpinfo=0&mth=GET
https://archibus.vodacom.co.za/_Incapsula_Resource?CWUDNSAI=23&xinfo=9-87395359-0%200NNN%20RT%2816998157396 49%2013%29%20q%280%20-1%20-1%20-1%29%20r
%280%20-1%29%20B15%284%2C200%2C0%29%20U18&incident_id=766001190516980779-491098904410856905&edet=15&cinfo=04000000&rpinfo=0&mth=GET
https://archibus.vodacom.co.za/_Incapsula_Resource?CWUDNSAI=23&xinfo=9-91007908-0%200NNN%20RT%2816919532952 03%205%29%20q%280%20-1%20-1%20-1%29%20r
%280%20-1%29%20B15%284%2c200%2c0%29%20U18&incident_id=128000730324386403-452294428900463177&edet=15&cinfo=04000000&rpinfo=0&mth=GET
https://archibus.vodacom.co.za/_Incapsula_Resource?SWKMTFSR=1&e=0.10408580974368586
https://archibus.vodacom.co.za/_Incapsula_Resource?SWKMTFSR=1&e=0.20939986879542816
https://archibus.vodacom.co.za/_Incapsula_Resource?SWKMTFSR=1&e=0.3450785737536535
https://archibus.vodacom.co.za/_Incapsula_Resource?SWKMTFSR=1&e=0.5272987180813904
https://archibus.vodacom.co.za/_Incapsula_Resource?SWKMTFSR=1&e=0.657332483118807
https://archibus.vodacom.co.za/_Incapsula_Resource?SWKMTFSR=1&e=0.748959364503075
https://archibus.vodacom.co.za/_Incapsula_Resource?SWKMTFSR=1&e=0.8762218735550797
https://archibus.vodacom.co.za/_Incapsula_Resource?SWKMTFSR=1&e=0.9411161046872494
https://archibus.vodacom.co.za/archibus/
https://archibus.vodacom.co.za/archibus/null
https://archibus.vodacom.co.za/csp_report
https://archibus.vodacom.co.za/docs/
https://archibus.vodacom.co.za/docs/RELEASE-NOTES.txt
https://archibus.vodacom.co.za/docs/api/
https://archibus.vodacom.co.za/docs/api/index.html
https://archibus.vodacom.co.za/docs/appdev/
https://archibus.vodacom.co.za/docs/changelog.html
https://archibus.vodacom.co.za/docs/cluster-howto.html
https://archibus.vodacom.co.za/docs/config/
https://archibus.vodacom.co.za/docs/deployer-howto.html
https://archibus.vodacom.co.za/docs/jndi-datasource-examples-howto.html
https://archibus.vodacom.co.za/docs/manager-howto.html
https://archibus.vodacom.co.za/docs/realm-howto.html
https://archibus.vodacom.co.za/docs/security-howto.html
https://archibus.vodacom.co.za/docs/setup.html
https://archibus.vodacom.co.za/examples/
https://archibus.vodacom.co.za/favicon.ico
https://archibus.vodacom.co.za/host-manager/
https://archibus.vodacom.co.za/host-manager/html
https://archibus.vodacom.co.za/manager/
https://archibus.vodacom.co.za/manager/html
https://archibus.vodacom.co.za/manager/status
https://archibus.vodacom.co.za/null

150010 External Links Discovered (1)

150010 External Links Discovered

archibus.vodacom.co.za/archibus

Finding #	10510598	**Severity**	Information Gathered - Level 1
Unique #	464213f9-af1d-465f-97e0-7ba33acea1ef		
Group	Scan Diagnostics		
CWE	-	**Detection Date**	11 Feb 2024 21:02 GMT+0200
OWASP	-		

WASC	-

Details

Threat
External links discovered during the scan are listed in the Results section. These links were out of scope for the scan and were not crawled.

Impact
N/A

Solution
N/A

Results

Number of links: 40
https://www.imperva.com/why-am-i-seeing-this-page/?src=23%22utm_source=blockingpages
https://www.imperva.com/why-am-i-seeing-this-page/?src=23&utm_source=blockingpages
https://github.com/apache/tomcat/tree/9.0.x
https://fonts.gstatic.com/s/inter/v13/UcC73FwrK3iLTeHuS_fvQtMwCp50KnMa1ZL7.woff2
https://fonts.googleapis.com/css2?family=Inter:wght@300;400;500;700%22display=swap
https://fonts.googleapis.com/css2?family=Inter:wght@300;400;500;700&display=swap
https://login.sso.vodacom.co.za/Hircannot-sleepetings-bottemper-Not-yourse-peaks
https://login.sso.vodacom.co.za/Hircannot-sleepetings-bottemper-Not-yourse-peaks?d=login.sso.vodacom.co.za
https://login.sso.vodacom.co.za/_Incapsula_Resource?CWUDNSAI=23&xinfo=42-8775126-0%200NNN%20RT%281707678198347%204%29%20q%280%20-1%20-1%20-1%29%20r%280%20-1%29%20B15%2811%2C2006056%2C0%29%20U18&incident_id=1687000190184622692-476066502750384 42&edet=15&cinfo=0b000000&rpinfo=0&mth=GET
https://login.sso.vodacom.co.za/_Incapsula_Resource?SWJIYLWA=719d34d31c8e3a6e6fffd425f7e032f3
https://login.sso.vodacom.co.za/_Incapsula_Resource?SWKMTFSR=1&e=0.23493708276474634
https://login.sso.vodacom.co.za/csp_report
https://login.sso.vodacom.co.za/favicon.ico
https://login.sso.vodacom.co.za/nidp/saml2/idpsend?id=archibus
https://wiki.apache.org/tomcat/FrontPage
https://wiki.apache.org/tomcat/Specifications
https://wiki.apache.org/tomcat/TomcatVersions
https://tomcat.apache.org/
https://tomcat.apache.org/bugreport.html
https://tomcat.apache.org/connectors-doc/
https://tomcat.apache.org/contact.html
https://tomcat.apache.org/download-connectors.cgi
https://tomcat.apache.org/download-native.cgi
https://tomcat.apache.org/faq/
https://tomcat.apache.org/findhelp.html
https://tomcat.apache.org/getinvolved.html
https://tomcat.apache.org/heritage.html
https://tomcat.apache.org/legal.html
https://tomcat.apache.org/lists.html
https://tomcat.apache.org/migration.html
https://tomcat.apache.org/native-doc/
https://tomcat.apache.org/resources.html
https://tomcat.apache.org/security.html
https://tomcat.apache.org/source.html
https://tomcat.apache.org/taglibs/
https://tomcat.apache.org/whoweare.html
https://www.apache.org/
https://www.apache.org/foundation/sponsorship.html
https://www.apache.org/foundation/thanks.html
http://go.microsoft.com/fwlink/?linkid=66138%22clcid%3D0x409

150020 Links Rejected By Crawl Scope or Exclusion List (1)

150020 Links Rejected By Crawl Scope or Exclusion List — *archibus.vodacom.co.za/archibus*

Finding #	10510585	Severity	Information Gathered - Level 1
Unique #	89df0ac9-0ebf-4c90-819a-0d45e2930ad6		
Group	Scan Diagnostics		
CWE	-	Detection Date	11 Feb 2024 21:02 GMT+0200
OWASP	-		
WASC	-		

Details

Threat
One or more links were not crawled because of an explicit rule to exclude them. This also occurs if a link is malformed.

Exclude list and Include list entries can cause links to be rejected. If a scan is limited to a specific starting directory, then links outside that directory will neither be crawled or tested.

Links that contain a host name or IP address different from the target application are considered external links and not crawled by default; those types of links are not listed here. This often happens when the scope of a scan is limited to the directory of the starting URL. The scope can be changed in the Web Application Record.

During the test phase, some path-based tests may be rejected if the scan is limited to the directory of the starting URL and the test would fall outside that directory. In these cases, the number of rejected links may be too high to list in the Results section.

Impact
Links listed here were neither crawled or tested by the Web application scanning engine.

Solution
A link might have been intentionally matched by a exclude or include list entry. Verify that no links in this list were unintentionally rejected.

Results

Links not permitted:
(This list includes links from QIDs: 150010,150041,150143,150170)

External links discovered:
https://www.imperva.com/why-am-i-seeing-this-page/?src=23%22utm_source=blockingpages
https://www.imperva.com/why-am-i-seeing-this-page/?src=23&utm_source=blockingpages
https://github.com/apache/tomcat/tree/9.0.x
https://fonts.gstatic.com/s/inter/v13/UcC73FwrK3iLTeHuS_fvQtMwCp50KnMa1ZL7.woff2
https://fonts.googleapis.com/css2?family=Inter:wght@300;400;500;700%22display=swap
https://fonts.googleapis.com/css2?family=Inter:wght@300;400;500;700&display=swap
https://login.sso.vodacom.co.za/Hircannot-sleepetings-bottemper-Not-yourse-peaks
https://login.sso.vodacom.co.za/Hircannot-sleepetings-bottemper-Not-yourse-peaks?d=login.sso.vodacom.co.za
https://login.sso.vodacom.co.za/_Incapsula_Resource?CWUDNSAI=23&xinfo=42-8775126-0%200NNN%20RT%281707678198347%204%29%20q%280%20-1%20-1%20-1%29%20r%280%20-1%29%20B15%2811%2C2006056%2C0%29%20U18&incident_id=1687000190184622692-476066502750384 42&edet=15&cinfo=0b000000&rpinfo=0&mth=GET
https://login.sso.vodacom.co.za/_Incapsula_Resource?SWJIYLWA=719d34d31c8e3a6e6fffd425f7e032f3

IP based excluded links:
Links rejected during the test phase not reported due to volume of links.

150021 Scan Diagnostics (1)

150021 Scan Diagnostics — *archibus.vodacom.co.za/archibus*

Finding #	10510586	**Severity**	Information Gathered - Level 1
Unique #	f650cbbb-c9d5-45ff-9361-477991eba13b		
Group	Scan Diagnostics		
CWE	-	**Detection Date**	11 Feb 2024 21:02 GMT+0200
OWASP	-		
WASC	-		

Details

Threat
This check provides various details of the scan's performance and behavior. In some cases, this check can be used to identify problems that the scanner encountered when crawling the target Web application.

Impact

The scan diagnostics data provides technical details about the crawler's performance and behavior. This information does not necessarily imply problems with the Web application.

Solution

No action is required.

Results

Loaded 4 exclude list entries.
Loaded 0 allow list entries.
HTML form authentication unavailable, no WEBAPP entry found
Target web application page https://archibus.vodacom.co.za/archibus/ fetched. Status code:302, Content-Type:text/html, load time:1 milliseconds.
Batch #0 VirtualHostDiscovery: estimated time < 10 minutes (70 tests, 0 inputs)
VirtualHostDiscovery: 70 vulnsigs tests, completed 70 requests, 713 seconds. Completed 70 requests of 70 estimated requests (100%). All tests completed.
Batch #0 SameSiteScripting: estimated time < 1 minute (2 tests, 0 inputs)
SameSiteScripting: 2 vulnsigs tests, completed 2 requests, 0 seconds. Completed 2 requests of 2 estimated requests (100%). All tests completed.
Batch #0 CMSDetection: estimated time < 10 minutes (1 tests, 1 inputs)
[CMSDetection phase] : No potential CMS found using Blind Elephant algorithm. Aborting the CMS Detection phase
CMSDetection: 1 vulnsigs tests, completed 56 requests, 23 seconds. Completed 56 requests of 56 estimated requests (100%). All tests completed.
No more requeues, redundant link threshold has been surpassed.
Collected 144 links overall in 0 hours 27 minutes duration.
Batch #0 BannersVersionReporting: estimated time < 1 minute (1 tests, 1 inputs)
BannersVersionReporting: 1 vulnsigs tests, completed 0 requests, 0 seconds. Completed 0 requests of 1 estimated requests (0%). All tests completed.
Path manipulation: Estimated requests (payloads x links): files with extension:(0 x 12) + files:(0 x 101) + directories:(9 x 10) + paths:(0 x 111) = total (90)
Batch #0 WS Directory Path manipulation: estimated time < 1 minute (9 tests, 111 inputs)
WS Directory Path manipulation: 9 vulnsigs tests, completed 90 requests, 5 seconds. Completed 90 requests of 90 estimated requests (100%). All tests completed.
Batch #0 WS enumeration: estimated time < 10 minutes (11 tests, 111 inputs)
WS enumeration: 11 vulnsigs tests, completed 211 requests, 305 seconds. Completed 211 requests of 1221 estimated requests (17.2809%). All tests completed.
Batch #1 URI parameter manipulation (no auth): estimated time < 10 minutes (125 tests, 16 inputs)
Batch #1 URI parameter manipulation (no auth): 125 vulnsigs tests, completed 1922 requests, 323 seconds. Completed 1922 requests of 2000 estimated requests (96.1%). Some tests were skipped due to errors.
Batch #1 URI parameter name manipulation (no auth): estimated time < 10 minutes (125 tests, 16 inputs)
Batch #1 URI parameter name manipulation (no auth): 125 vulnsigs tests, completed 369 requests, 1 seconds. Completed 369 requests of 2000 estimated requests (18.45%). All tests completed.
Batch #1 URI blind SQL manipulation (no auth): estimated time < 1 minute (13 tests, 16 inputs)
Batch #1 URI blind SQL manipulation (no auth): 13 vulnsigs tests, completed 481 requests, 1 seconds. Completed 481 requests of 624 estimated requests (77.0833%). All tests completed.
Batch #1 URI parameter time-based tests (no auth): estimated time < 1 minute (19 tests, 16 inputs)
Batch #1 URI parameter time-based tests (no auth): 19 vulnsigs tests, completed 304 requests, 1 seconds. Completed 304 requests of 304 estimated requests (100%). All tests completed.
Batch #1 URI parameter time-based tests for Apache Struts Vulnerabilities (no auth): estimated time < 1 minute (1 tests, 16 inputs)
Batch #1 URI parameter time-based tests for Apache Struts Vulnerabilities (no auth): 1 vulnsigs tests, completed 16 requests, 0 seconds. Completed 16 requests of 16 estimated requests (100%). All tests completed.
Batch #4 WebCgiOob: estimated time < 10 minutes (133 tests, 1 inputs)
Batch #4 WebCgiOob: 133 vulnsigs tests, completed 53 requests, 400 seconds. Completed 53 requests of 17205 estimated requests (0.30805%). All tests completed.
No XML requests found. Skipping XXE tests.
Batch #4 DOM XSS exploitation: estimated time < 1 minute (4 tests, 0 inputs)
Batch #4 DOM XSS exploitation: 4 vulnsigs tests, completed 0 requests, 1 seconds. No tests to execute.
Batch #4 HTTP call manipulation: estimated time < 1 minute (59 tests, 0 inputs)
Batch #4 HTTP call manipulation: 59 vulnsigs tests, completed 0 requests, 0 seconds. No tests to execute.
Batch #4 Open Redirect analysis: estimated time < 1 minute (2 tests, 1 inputs)
Batch #4 Open Redirect analysis: 2 vulnsigs tests, completed 2 requests, 12 seconds. Completed 2 requests of 2 estimated requests (100%). All tests completed.
CSRF tests will not be launched because the scan is not successfully authenticated.
Batch #4 File Inclusion analysis: estimated time < 1 minute (1 tests, 114 inputs)
Batch #4 File Inclusion analysis: 1 vulnsigs tests, completed 0 requests, 0 seconds. Completed 0 requests of 114 estimated requests (0%). All tests completed.
Batch #4 Cookie manipulation: estimated time < 10 minutes (76 tests, 4 inputs)
Batch #4 Cookie manipulation: 76 vulnsigs tests, completed 5290 requests, 640 seconds. Completed 5290 requests of 5200 estimated requests (101.731%). XSS optimization removed 2500 links. All tests completed.
Batch #4 Header manipulation: estimated time < 30 minutes (76 tests, 50 inputs)
Batch #4 Header manipulation: 76 vulnsigs tests, completed 10000 requests, 607 seconds. Completed 10000 requests of 20400 estimated requests (49.0196%). XSS optimization removed 2500 links. All tests completed.
Batch #4 shell shock detector: estimated time < 1 minute (1 tests, 50 inputs)
Batch #4 shell shock detector: 1 vulnsigs tests, completed 52 requests, 1 seconds. Completed 52 requests of 50 estimated requests (104%). All tests completed.
Batch #4 shell shock detector(form): estimated time < 1 minute (1 tests, 0 inputs)
Batch #4 shell shock detector(form): 1 vulnsigs tests, completed 0 requests, 0 seconds. No tests to execute.
Login Brute Force manipulation estimated time: no tests enabled
Login Brute Force manipulation estimated time: no tests enabled
Batch #5 HTTP Time Bandit: estimated time < 1 minute (1 tests, 10 inputs)
Batch #5 HTTP Time Bandit: 1 vulnsigs tests, completed 200 requests, 9 seconds. No tests to execute.
Path manipulation: Estimated requests (payloads x links): files with extension:(1 x 12) + files:(0 x 101) + directories:(4 x 10) + paths:(14 x 111) = total (1606)
Batch #5 Path XSS manipulation: estimated time < 1 minute (19 tests, 111 inputs)
Batch #5 Path XSS manipulation: 19 vulnsigs tests, completed 474 requests, 1 seconds. Completed 474 requests of 1606 estimated requests (29.5143%). All tests completed.
Path manipulation: Estimated requests (payloads x links): files with extension:(0 x 12) + files:(0 x 101) + directories:(1 x 10) + paths:(0 x 111) = total (10)
Batch #5 Tomcat Vuln manipulation: estimated time < 1 minute (1 tests, 111 inputs)
Batch #5 Tomcat Vuln manipulation: 1 vulnsigs tests, completed 9 requests, 0 seconds. Completed 9 requests of 10 estimated requests (90%). All tests completed.
Path manipulation: Estimated requests (payloads x links): files with extension:(0 x 12) + files:(0 x 101) + directories:(16 x 10) + paths:(0 x 111) = total (160)
Batch #5 Time based path manipulation: estimated time < 1 minute (16 tests, 114 inputs)
Batch #5 Time based path manipulation: 16 vulnsigs tests, completed 96 requests, 0 seconds. Completed 96 requests of 160 estimated requests (60%). All tests completed.
Path manipulation: Estimated requests (payloads x links): files with extension:(4 x 12) + files:(18 x 101) + directories:(152 x 10) + paths:(19 x 111) = total (5495)
Batch #5 Path manipulation: estimated time < 10 minutes (193 tests, 111 inputs)
Batch #5 Path manipulation: 193 vulnsigs tests, completed 2023 requests, 93 seconds. Completed 2023 requests of 5495 estimated requests (36.8153%). All tests completed.

Batch #5 WebCgiHrs: estimated time < 1 minute (1 tests, 1 inputs)
Batch #5 WebCgiHrs: 1 vulnsigs tests, completed 6 requests, 0 seconds. Completed 6 requests of 222 estimated requests (2.7027%). All tests completed.
Batch #5 WebCgiGeneric: estimated time < 1 hour (451 tests, 1 inputs)
Batch #5 WebCgiGeneric: 451 vulnsigs tests, completed 8278 requests, 656 seconds. Completed 8278 requests of 67155 estimated requests (12.3267%). All tests completed.
Batch #5 Open Redirect analysis: estimated time < 1 minute (2 tests, 1 inputs)
Batch #5 Open Redirect analysis: 2 vulnsigs tests, completed 0 requests, 5 seconds. Completed 0 requests of 2 estimated requests (0%). All tests completed.
Duration of Crawl Time: 1620.00 (seconds)
Duration of Test Phase: 3463.00 (seconds)
Total Scan Time: 5083.00 (seconds)

Total requests made: 31092
Average server response time: 0.18 seconds

Average browser load time: 0.17 seconds

150028 Cookies Collected (1)

150028 Cookies Collected

archibus.vodacom.co.za/archibus

Finding #	10510591	**Severity**	Information Gathered - Level 1
Unique #	5cdb06dd-9a23-49a0-9d32-c3ded137e768		
Group	Scan Diagnostics		
CWE	-	**Detection Date**	11 Feb 2024 21:02 GMT+0200
OWASP	-		
WASC	-		

Details

Threat
The cookies listed in the Results section were set by the web application during the crawl phase.

Impact
Cookies may potentially contain sensitive information about the user.

Note: Long scan duration can occur if a web application sets a large number of cookies (e.g., 25 cookies or more) and QIDs 150002, 150046, 150047, and 150048 are enabled.

Solution
Review cookie values to ensure they do not include sensitive information. If scan duration is excessive due to a large number of cookies, consider excluding QIDs 150002, 150046, 150047, and 150048.

Results

Total cookies: 7
visid_incap_2776849=2mCPlvHbTaSKgOs2WBZQC/YZyWUAAAAAQUIPAAAAAAAWwMvjPe13zMYdphiXlTQy; HttpOnly; expires=Sun, 09-Feb-2025 22:21:11 GMT; domain=.vodacom.co.za; path=/ First set at URL: https://archibus.vodacom.co.za/archibus/
nlbi_2776849=ogi1WuqyhRkuEuYJZU49BAAAAABLcyLrdKjEmQdibbXYNFmh; domain=.vodacom.co.za; path=/ First set at URL: https://archibus.vodacom.co.za/archibus/
incap_ses_1687_2776849=9uxXXci+jlSe7PgfvG1pF/YZyWUAAAAAfr+BmEPjvWAiYHFjqA+aDQ==; domain=.vodacom.co.za; path=/ First set at URL: https://archibus.vodacom.co.za/archibus/
visid_incap_2653607=5WyHTAoQTwOQASGxHqHFwPYZyWUAAAAAQUIPAAAAAAAv++5Sd7WI0erJwGETz3BS; HttpOnly; expires=Sun, 09-Feb-2025 22:21:08 GMT; domain=.sso.vodacom.co.za; path=/ First set at URL: https://archibus.vodacom.co.za/archibus/
incap_ses_1687_2653607=pVjWcBFg02Oo7PgfvG1pF/YZyWUAAAAAI+PNsdwCbDKGdroEybsU0w==; domain=.sso.vodacom.co.za; path=/ First set at URL: https://archibus.vodacom.co.za/archibus/
nlbi_2653607_2147483392=ph9bJJxIAXaVCw2VoHFvpQAAAAAk8dnUexHo3DCUpnHVyO/T; domain=.sso.vodacom.co.za; path=/ First set at URL: https://archibus.vodacom.co.za/archibus/
nlbi_2776849_2147483392=XMT0KRDY20D/IVChZU49BAAAAAA352epqdF/yOosCbwaXEXg; domain=.vodacom.co.za; path=/ First set at URL: https://archibus.vodacom.co.za/FPRWin/index.aspx

150097 HTTP Response Indicates Scan May Be Blocked (1)

150097 HTTP Response Indicates Scan May Be Blocked

archibus.vodacom.co.za/archibus

Finding #	10510594	**Severity**	Information Gathered - Level 1
Unique #	2c6a9645-43a8-4f1a-8ed4-0eb229fdf27a		

WAS Web Application Report

Group	Scan Diagnostics		
CWE	-	**Detection Date**	11 Feb 2024 21:02 GMT+0200
OWASP	-		
WASC	-		

Details

Threat

The scanner received an HTTP response from the target web site that contains a message indicating the scan has been blocked. This often occurs due to an intermediate security device such as a web application firewall (WAF), intrusion detection system (IDS), or intrusion prevention system (IPS).

Impact

If the scanner's IP or traffic has been blocked, then the results of the scan will be empty or incomplete because the web site could not be successfully crawled and tested.

Solution

Modify relevant security rules so that the WAS scans will not trigger alerts or be otherwise blocked. Additionally, review 150528 for additional HTTP 4XX Error Code responses found during the scanning.

Results

Uri: https://archibus.vodacom.co.za/_Incapsula_Resource?CWUDNSAI=23&xinfo=13-50005422-0%200NNN%20RT%281684091004823%2015780%29%20q%280%20-1%20-1%201%29%20r%280%20-1%29%20B15%284%2C200%2C0%29%20U18&incident_id=768000330126840138-244105402621364301&edet=15&cinfo=04000000&rpinfo=0&mth=GET
Match: pan>

Powered by
Imperva

</body></html>

Uri: https://archibus.vodacom.co.za/_Incapsula_Resource?CWUDNSAI=23&xinfo=13-51475397-0%200NNN%20RT%281696791744809%2015891%29%20q%280%20-1%20-1%200%29%20r%280%20-1%29%20B15%284%2C200%2C0%29%20U18&incident_id=764000460129603047-262001204198640525&edet=15&cinfo=04000000&rpinfo=0&mth=GET
Match: pan>

Powered by
Imperva

</body></html>

Uri: https://archibus.vodacom.co.za/_Incapsula_Resource?CWUDNSAI=23&xinfo=13-51475396-0%200NNN%20RT%281696791744809%202625%29%20q%280%20-1%20-1%202%29%20r%280%20-1%29%20B15%284%2C200%2C0%29%20U18&incident_id=764000460129603047-261986575540030349&edet=15&cinfo=04000000&rpinfo=0&mth=GET
Match: pan>

Powered by
Imperva

</body></html>

Uri: https://archibus.vodacom.co.za/_Incapsula_Resource?CWUDNSAI=23&xinfo=14-178098704-0%200NNN%20RT%281681066855737%202281%29%20q%280%20-1%20-1%208%29%20r%280%20-1%29%20B15%284%2C200%2C0%29%20U18&incident_id=766000980317811993-862742334339422350&edet=15&cinfo=04000000&rpinfo=0&mth=GET
Match: pan>

Powered by
Imperva

</body></html>

Uri: https://archibus.vodacom.co.za/_Incapsula_Resource?CWUDNSAI=23&xinfo=14-178100241-0%200NNN%20RT%281681066864525%202%29%20q%280%20-1%20-1%200%29%20r%280%20-1%29%20B15%284%2c200%2c0%29%20U18&incident_id=766000980317811993-862747269256845454&edet=15&cinfo=04000000&rpinfo=0&mth=GET
Match: pan>

Powered by
Imperva

</body></html>

Uri: https://archibus.vodacom.co.za/_Incapsula_Resource?CWUDNSAI=23&xinfo=14-56552041-0%200NNN%20RT%281684091004822%202271%29%20q%280%20-1%20-1%200%29%20r%280%20-1%29%20B15%284%2C200%2C0%29%20U18&incident_id=768000330126840138-290605261188499534&edet=15&cinfo=04000000&rpinfo=0&mth=GET
Match: pan>

Powered by
Imperva

</body></html>

Uri: https://archibus.vodacom.co.za/_Incapsula_Resource?CWUDNSAI=23&xinfo=14-178098704-0%200NNN%20RT%281681066855737%202281%29%20q%280%20-1%20-1%208%29%20r%280%20-1%29%20B15%284%2c200%2c0%29%20U18&incident_id=766000980317811993-862742334339422350&edet=15&cinfo=04000000&rpinfo=0&mth=GET
Match: pan>

Powered by
Imperva

</body></html>

Uri: https://archibus.vodacom.co.za/_Incapsula_Resource?CWUDNSAI=23&xinfo=14-99580654-0%200NNN%20RT%2816943725251 49%204%29%20q%280%20-1%20-1%200%29%20r%280%20-1%29%20B15%284%2c200%2c0%29%20U18&incident_id=764000410179907764-464701605912775246&edet=15&cinfo=04000000&rpinfo=0&mth=GET
Match: pan>

Powered by
Imperva

</body></html>

Uri: https://archibus.vodacom.co.za/_Incapsula_Resource?CWUDNSAI=23&xinfo=14-99576411-0%200NNN%20RT%281694372512606%209%29%20q%280%20-1%20-1%20-1%29%20r%280%20-1%29%20B15%284%2c200%2c0%29%20U18&incident_id=764000410179907764-464681797523606094&edet=15&cinfo=04000000&rpinfo=0&mth=GET
Match: pan>

Powered by
Imperva

</body></html>

Uri: https://archibus.vodacom.co.za/_Incapsula_Resource?CWUDNSAI=23&xinfo=4-185001335-0%200NNN%20RT%2816888929350663%207%29%20q%280%20-1%20-1%20-1%29%20r%280%20-1%29%20B15%284%2c200%2c0%29%20U18&incident_id=449001580571594800-9499091938071776 04&edet=15&cinfo=04000000&rpinfo=0&mth=GET
Match: pan>

Powered by
Imperva

</body></html>

Uri: https://archibus.vodacom.co.za/_Incapsula_Resource?CWUDNSAI=23&xinfo=4-6583483-0%200NNN%20RT%2816967916769 41%203%29%20q%280%20-1%20-1%20-1%29%20r%280%20-1%29%20B15%284%2c200%2c0%29%20U18&incident_id=764000460129603047-34059786492054404&edet=15&cinfo=04000000&rpinfo=0&mth=GET
Match: pan>

Powered by
Imperva

</body></html>

Uri: https://archibus.vodacom.co.za/_Incapsula_Resource?CWUDNSAI=23&xinfo=4-9346511-0%200NNN%20RT%2816943725160 64%2015875%29%20q%280%20-1%20-1%200%29%20r%280%20-1%29%20B15%284%2C200%2C0%29%20U18&incident_id=764000410179907764-456022061573760 68&edet=15&cinfo=04000000&rpinfo=0&mth=GET
Match: pan>

Powered by
Imperva

</body></html>

Uri: https://archibus.vodacom.co.za/_Incapsula_Resource?CWUDNSAI=23&xinfo=4-77155952-0%200NNN%20RT%281699815748753%203%29%20q%280%20-1%20-1%200%29%20r%280%20-1%29%20B15%284%2c200%2c0%29%20U18&incident_id=766001190516980779-434236724277550532&edet=15&cinfo=04000000&rpinfo=0&mth=GET
Match: pan>

Powered by
Imperva

</body></html>

Uri: https://archibus.vodacom.co.za/_Incapsula_Resource?CWUDNSAI=23&xinfo=5-218374445-0%200NNN%20RT%2816889294634 09%203%29%20q%280%20-1%20-1%200%29%20r%280%20-1%29%20B15%284%2c200%2c0%29%20U18&incident_id=449001580571594800-111896152893929 2549&edet=15&cinfo=04000000&rpinfo=0&mth=GET
Match: pan>

Powered by
Imperva

</body></html>

Uri: https://archibus.vodacom.co.za/_Incapsula_Resource?CWUDNSAI=23&xinfo=5-102401836-0%200NNN%20RT%2816865104846 94%203%29%20q%280%20-1%20-1%20-1%29%20r%280%20-1%29%20B15%284%2c200%2c0%29%20U18&incident_id=769009803598071 66-486662297683564677&edet=15&cinfo=04000000&rpinfo=0&mth=GET
Match: pan>

Powered by
Imperva

</body></html>

Uri: https://archibus.vodacom.co.za/_Incapsula_Resource?CWUDNSAI=23&xinfo=5-218372829-0%200NNN%20RT%2816889294541 17%202786%29%20q%280%20-1%20-1%201%29%20r%280%20-1%29%20B15%284%2C200%2C0%29%20U18&incident_id=449001580571594800-111895544297063 4117&edet=15&cinfo=04000000&rpinfo=0&mth=GET
Match: pan>

Powered by
Imperva

</body></html>

Uri: https://archibus.vodacom.co.za/_Incapsula_Resource?CWUDNSAI=23&xinfo=6-50761907-0%200NNN%20RT%2816919534291 71%2013568%29%20q%280%20-1%20-1%200%29%20r%280%20-1%29%20B15%284%2C200%2C0%29%20U18&incident_id=128000730324386403-257296789038699078&edet=15&cinfo=04000000&rpinfo=0&mth=GET
Match: pan>

Powered by
Imperva

</body></html>

Uri: https://archibus.vodacom.co.za/_Incapsula_Resource?CWUDNSAI=23&xinfo=7-120841300-0%200NNN%20RT%281688929454097%2014%29%20q%280%20-1%20-1%20-1%29%20r%280%20-1%29%20B15%284%2C200%2C0%29%20U18&incident_id=449001580571594800-63172921613150810 3&edet=15&cinfo=04000000&rpinfo=0&mth=GET
Match: pan>

Powered by
Imperva

</body></html>

Uri: https://archibus.vodacom.co.za/_Incapsula_Resource?CWUDNSAI=23&xinfo=6-59075188-0%200NNN%20RT%281699815693202%203%29%20q%280%20-1%20-1%20-1%29%20r%280%20-1%29%20B15%284%2c200%2c0%29%20U18&incident_id=766001190516980779-333163456469278150&edet=15&cinfo=04000000&rpinfo=0&mth=GET
Match: pan>

Powered by
Imperva

</body></html>

Uri: https://archibus.vodacom.co.za/_Incapsula_Resource?CWUDNSAI=23&xinfo=9-31678237-0%200NNN%20RT%281684091013878%203%29%20q%280%20-1%20-1%201%29%20r%280%20-1%29%20B15%284%2c200%2c0%29%20U18&incident_id=768000330126840138-156191708449605705&edet=15&cinfo=04000000&rpinfo=0&mth=GET
Match: pan>

Powered by
Imperva

</body></html>

Uri: https://archibus.vodacom.co.za/_Incapsula_Resource?CWUDNSAI=23&xinfo=8-71777546-0%200NNN%20RT%281691953415895%209146%29%20q%280%20-1%20-1%202%29%20r%280%20-1%29%20B15%284%2C200%2C0%29%20U18&incident_id=128000730324386403-355359155923456584&edet=15&cinfo=04000000&rpinfo=0&mth=GET
Match: pan>

Powered by
Imperva

</body></html>

Uri: https://archibus.vodacom.co.za/_Incapsula_Resource?CWUDNSAI=23&xinfo=7-120841302-0%200NNN%20RT%281688929454119%2016073%29%20q%280%20-1%20-1%200%29%20r%280%20-1%29%20B15%284%2C200%2C0%29%20U18&incident_id=449001580571594800-631738012224530311&edet=15&cinfo=04000000&rpinfo=0&mth=GET
Match: pan>

Powered by
Imperva

</body></html>

Uri: https://archibus.vodacom.co.za/_Incapsula_Resource?CWUDNSAI=23&xinfo=9-91007908-0%200NNN%20RT%281691953295203%205%29%20q%280%20-1%20-1%20-1%29%20r%280%20-1%29%20B15%284%2c200%2c0%29%20U18&incident_id=128000730324386403-452294428900463177&edet=15&cinfo=04000000&rpinfo=0&mth=GET
Match: pan>

Powered by
Imperva

</body></html>

Uri: https://archibus.vodacom.co.za/_Incapsula_Resource?CWUDNSAI=23&xinfo=9-87395359-0%200NNN%20RT%281699815739649%2013%29%20q%280%20-1%20-1%20-1%29%20r%280%20-1%29%20B15%284%2C200%2C0%29%20U18&incident_id=766001190516980779-491098904410856905&edet=15&cinfo=04000000&rpinfo=0&mth=GET
Match: pan>

Powered by
Imperva

</body></html>

Uri: https://archibus.vodacom.co.za/_Incapsula_Resource?CWUDNSAI=23&xinfo=9-82952600-0%200NNN%20RT%281686510547426%2013%29%20q%280%20-1%20-1%20-1%29%20r%280%20-1%29%20B15%284%2C200%2C0%29%20U18&incident_id=769000980359807166-403616321876596873&edet=15&cinfo=04000000&rpinfo=0&mth=GET
Match: pan>

Powered by
Imperva

</body></html>

Uri: https://archibus.vodacom.co.za/_Incapsula_Resource?CWUDNSAI=23&xinfo=10-107502277-0%200NNN%20RT%281686510550324%2012994%29%20q%280%20-1%20-1%200%29%20r%280%20-1%29%20B15%284%2C200%2C0%29%20U18&incident_id=769000980359807166-5152181093055264l0&edet=15&cinfo=04000000&rpinfo=0&mth=GET
Match: pan>

Powered by
Imperva

</body></html>

Uri: https://archibus.vodacom.co.za/_Incapsula_Resource?CWUDNSAI=23&xinfo=10-112005025-0%200NNN%20RT%281691953408943%2013%29%20q%280%20-1%20-1%20-1%29%20r%280%20-1%29%20B15%284%2C200%2C0%29%20U18&incident_id=128000730324386403-546908765975220810&edet=15&cinfo=04000000&rpinfo=0&mth=GET
Match: pan>

Powered by
Imperva

</body></html>

Uri: https://archibus.vodacom.co.za/_Incapsula_Resource?CWUDNSAI=23&xinfo=10-112007274-0%200NNN%20RT%281691953418647%206%29%20q%280%20-1%20-1%200%29%20r%280%20-1%29%20B15%284%2c200%2c0%29%20U18&incident_id=128000730324386403-546919408904180298&edet=15&cinfo=04000000&rpinfo=0&mth=GET
Match: pan>

Powered by
Imperva

</body></html>

Uri: https://archibus.vodacom.co.za/_Incapsula_Resource?CWUDNSAI=23&xinfo=10-64315409-0%200NNN%20RT%281694372516043%2013%29%20q%280%20-1%20-1%20-1%29%20r%280%20-1%29%20B15%284%2C200%2C0%29%20U18&incident_id=764000410179907764-309217785433295434&edet=15&cinfo=04000000&rpinfo=0&mth=GET
Match: pan>

Powered by
Imperva

</body></html>

Uri: https://archibus.vodacom.co.za/_Incapsula_Resource?CWUDNSAI=23&xinfo=11-113096202-0%200NNN%20RT%281681066855738%2015577%29%20q%280%20-1%20-1%200%29%20r%280%20-1%29%20B15%284%2C200%2C0%29%20U18&incident_id=766000980317811993-551562440391661707&edet=15&cinfo=04000000&rpinfo=0&mth=GET
Match: pan>

Powered by
Imperva

</body></html>

Uri: https://archibus.vodacom.co.za/_Incapsula_Resource?CWUDNSAI=23&xinfo=11-128333115-0%200NNN%20RT%281686510547447%202871%29%20q%280%20-1%20-1%200%29%20r%280%20-1%29%20B15%284%2C200%2C0%29%20U18&incident_id=769000980359807166-612085775202326667&edet=15&cinfo=04000000&rpinfo=0&mth=GET
Match: pan>

Powered by
Imperva

</body></html>

Uri: https://archibus.vodacom.co.za/_Incapsula_Resource?CWUDNSAI=23&xinfo=11-113096202-0%200NNN%20RT%281681066855738%2015577%29%20q%280%20-1%20-1%200%29%20r%280%20-1%29%20B15%284%2c200%2c0%29%20U18&incident_id=766000980317811993-551562440391661707&edet=15&cinfo=04000000&rpinfo=0&mth=GET
Match: pan>

Powered by
Imperva

</body></html>

Uri: https://archibus.vodacom.co.za/_Incapsula_Resource?CWUDNSAI=23&xinfo=11-74601801-0%200NNN%20RT%2816943725160 63%202785%29%20q%280%20-1%20-1%200%29%20r%280%20-1%29%20B15%284%2C200%2C0%29%20U18&incident_id=764000410179907764-353379304890698315&edet=15&cinfo=04000000&rpinfo=0&mth=GET
Match: pan>

Powered by
Imperva

</body></html>

Uri: https://archibus.vodacom.co.za/_Incapsula_Resource?CWUDNSAI=23&xinfo=12-140568936-0%200NNN%20RT%2816999815739671%202292%29%20q%280%20-1%20-1%201%29%20r%280%20-1%29%20B15%284%2C200%2C0%29%20U18&incident_id=766001190516980779-773471142739320268&edet=15&cinfo=04000000&rpinfo=0&mth=GET
Match: pan>

Powered by
Imperva

</body></html>

Uri: https://archibus.vodacom.co.za/_Incapsula_Resource?CWUDNSAI=23&xinfo=12-134233322-0%200NNN%20RT%281681066855720%209%29%20q%280%20-1%20-1%20-1%29%20r%280%20-1%29%20B15%284%2C200%2C0%29%20U18&incident_id=766000980317811993-650986591082125452&edet=15&cinfo=04000000&rpinfo=0&mth=GET

Match: pan>

Powered by
Imperva

</body></html>

Uri: https://archibus.vodacom.co.za/_Incapsula_Resource?CWUDNSAI=23&xinfo=12-143394600-0%200NNN%20RT%281691953410996%20780%29%20q%280%20-1%20-1%200%29%20r%280%20-1%29%20B15%284%2C200%2C0%29%20U18&incident_id=128000730324386403-68869439385449735 6&edet=15&cinfo=04000000&rpinfo=0&mth=GET
Match: pan>

Powered by
Imperva

</body></html>

Uri: https://archibus.vodacom.co.za/_Incapsula_Resource?CWUDNSAI=23&xinfo=12-44624439-0%200NNN%20RT%281684091004803%2012%29%20q%280%20-1%20-1%20-1%29%20r%280%20-1%29%20B15%284%2C200%2C0%29%20U18&incident_id=768000330126840138-230990165932247116&edet=15&cinfo=04000000&rpinfo=0&mth=GET
Match: pan>

Powered by
Imperva

</body></html>

Uri: https://archibus.vodacom.co.za/_Incapsula_Resource?CWUDNSAI=23&xinfo=12-46623679-0%200NNN%20RT%281696791744790%2011%29%20q%280%20-1%20-1%20-1%29%20r%280%20-1%29%20B15%284%2C200%2C0%29%20U18&incident_id=764000460129603047-238669739255925644&edet=15&cinfo=04000000&rpinfo=0&mth=GET
Match: pan>

Powered by
Imperva

</body></html>

Uri: https://archibus.vodacom.co.za/_Incapsula_Resource?CWUDNSAI=23&xinfo=13-176129679-0%200NNN%20RT%281686510556626%204%29%20q%280%20-1%20-1%200%29%20r%280%20-1%29%20B15%284%2c200%2c0%29%20U18&incident_id=769000980359807166-833884303048906893&edet=15&cinfo=04000000&rpinfo=0&mth=GET
Match: pan>

Powered by

Imperva

</body></html>

Uri: https://archibus.vodacom.co.za/_Incapsula_Resource?CWUDNSAI=23&xinfo=12-46625623-0%200NNN%20RT%281696791754309%203%29%20q%280%20-1%20-1%201%29%20r%280%20-1%29%20B15%284%2c200%2c0%29%20U18&incident_id=764004601296030 47-238679617680706444&edet=15&cinfo=04000000&rpinfo=0&mth=GET
Match: pan>

Powered by
Imperva

</body></html>

Uri: https://archibus.vodacom.co.za/_Incapsula_Resource?CWUDNSAI=23&xinfo=13-133113832-0%200NNN%20RT%281699815739671%2015870%29%20q%280%20-1%20-1%200%29%20r%280%20-1%29%20B15%284%2C200%2C0%29%20U18&incident_id=7660011905169807 79-72822869168266 3885&edet=15&cinfo=04000000&rpinfo=0&mth=GET
Match: pan>

Powered by
Imperva

</body></html>

Uri: https://archibus.vodacom.co.za/_Incapsula_Resource?CWUDNSAI=23&xinfo=13-49979840-0%200NNN%20RT%281684090900225%203%29%20q%280%20-1%20-1%20-1%29%20r%280%20-1%29%20B15%284%2c200%2c0%29%20U18&incident_id=768000330126840138-2439719622824448 77&edet=15&cinfo=04000000&rpinfo=0&mth=GET
Match: pan>

Powered by
Imperva

</body></html>

Uri: https://archibus.vodacom.co.za/_Incapsula_Resource?CWUDNSAI=23&xinfo=14-126467959-0%200NNN%20RT%2817022349285 13%2014%29%20q%280%20-1%20-1%20-1%29%20r%280%20-1%29%20B15%284%2C200%2C0%29%20U18&incident_id=770001170436975887-660755094765182286&edet=15&cinfo=04000000&rpinfo=0&mth=GET
Match: pan>

Powered by
Imperva

</body></html>

Uri: https://archibus.vodacom.co.za/_Incapsula_Resource?CWUDNSAI=23&xinfo=37-6345043-0%200NNN%20RT%2817052589995 33%2016038%29%20q%280%20-1%20-1%200%29%20r

%280%20-1%29%20B15%284%2C200%2C0%29%20U18&incident_id=1688000050322087314-40738971798995301&edet=15&cinfo=04000000&rpinfo=0&mth=GET
Match: pan>

Powered by
Imperva

</body></html>

Uri: https://archibus.vodacom.co.za/_Incapsula_Resource?CWUDNSAI=23&xinfo=36-7073891-0%200NNN%20RT%281705258999531%202780%29%20q%280%20-1%20-1%200%29%20r%280%20-1%29%20B15%284%2C200%2C0%29%20U18&incident_id=1688000050322087314-44942628090282340&edet=15&cinfo=04000000&rpinfo=0&mth=GET
Match: pan>

Powered by
Imperva

</body></html>

Uri: https://archibus.vodacom.co.za/_Incapsula_Resource?CWUDNSAI=23&xinfo=16-2346944-0%200NNN%20RT%281705258999514%2010%29%20q%280%20-1%20-1%20-1%29%20r%280%20-1%29%20B15%284%2C200%2C0%29%20U18&incident_id=1688000050322087314-16147372041568592&edet=15&cinfo=04000000&rpinfo=0&mth=GET
Match: pan>

Powered by
Imperva

</body></html>

Uri: https://archibus.vodacom.co.za/_Incapsula_Resource?CWUDNSAI=23&xinfo=5-85633350-0%200NNN%20RT%281702234935613%208793%29%20q%280%20-1%20-1%200%29%20r%280%20-1%29%20B15%284%2C200%2C0%29%20U18&incident_id=770001170436975887-430458772260003141&edet=15&cinfo=04000000&rpinfo=0&mth=GET
Match: pan>

Powered by
Imperva

</body></html>

Uri: https://archibus.vodacom.co.za/_Incapsula_Resource?CWUDNSAI=23&xinfo=57-14510035-0%200NNN%20RT%281705258916770%204%29%20q%280%20-1%20-1%20-1%29%20r%280%20-1%29%20B15%284%2c200%2c0%29%20U18&incident_id=1688000050322087314-90567331236282745&edet=15&cinfo=04000000&rpinfo=0&mth=GET
Match: pan>

Powered by
Imperva

</body></html>

Uri: https://archibus.vodacom.co.za/_Incapsula_Resource?CWUDNSAI=23&xinfo=5-85625692-0%200NNN%20RT%281702234865969%203%29%20q%280%20-1%20-1%20-1%29%20r%280%20-1%29%20B15%284%2c200%2c0%29%20U18&incident_id=770001170436975887-430417836926704965&edet=15&cinfo=04000000&rpinfo=0&mth=GET
Match: pan>

Powered by
Imperva

</body></html>

Uri: https://archibus.vodacom.co.za/_Incapsula_Resource?CWUDNSAI=23&xinfo=7-2288043-0%200NNN%20RT%281705259009181%203%29%20q%280%20-1%20-1%201%29%20r%280%20-1%29%20B15%284%2c200%2c0%29%20U18&incident_id=1688000050322087314-16354303565889863&edet=15&cinfo=04000000&rpinfo=0&mth=GET
Match: pan>

Powered by
Imperva

</body></html>

Uri: https://archibus.vodacom.co.za/_Incapsula_Resource?CWUDNSAI=23&xinfo=13-115516529-0%200NNN%20RT%281702234937715%206%29%20q%280%20-1%20-1%200%29%20r%280%20-1%29%20B15%284%2c200%2c0%29%20U18&incident_id=770001170436975887-61088416790702420 5&edet=15&cinfo=04000000&rpinfo=0&mth=GET
Match: pan>

Powered by
Imperva

</body></html>

Uri: https://archibus.vodacom.co.za/_Incapsula_Resource?CWUDNSAI=23&xinfo=7-74746777-0%200NNN%20RT%281702234928535%202882%29%20q%280%20-1%20-1%200%29%20r%280%20-1%29%20B15%284%2C200%2C0%29%20U18&incident_id=770001170436975887-376282892306881863&edet=15&cinfo=04000000&rpinfo=0&mth=GET
Match: pan>

Powered by
Imperva

</body></html>

Uri: https://archibus.vodacom.co.za/_Incapsula_Resource?CWUDNSAI=23&xinfo=9-67061412-0%200NNN%20RT%281681066852139%207%29%20q%280%20-1%20-1%20-1%29%20r%280%20-1%29%20B15%284%2c200%2c0%29%20U18&incident_id=766000980317811993-326349297580644489&edet=15&cinfo=04000000&rpinfo=0&mth=GET
Match: pan>

Powered by
Imperva

</body></html>

Uri: https://archibus.vodacom.co.za/_Incapsula_Resource?CWUDNSAI=23&xinfo=9-67061412-0%200NNN%20RT%281681066852139%207%29%20q%280%20-1%20-1%20-1%29%20r%280%20-1%29%20B15%284%2c200%2c0%29%20U18&incident_id=766000980317811993-326349297580644489&edet=15&cinfo=04000000&rpinfo=0&mth=GET
Match: pan>

Powered by
Imperva

</body></html>

Total 1153 request(s) were blocked by WAF/IPS/Firewall during path manipulation testing.Total 1153 request(s) were blocked by WAF/IPS/Firewall during path manipulation testing.Total 1153 request(s) were blocked by WAF/IPS/Firewall during path manipulation testing.Total 1153 request(s) were blocked by WAF/IPS/Firewall during path manipulation testing.Total 1153 request(s) were blocked by WAF/IPS/Firewall during path manipulation testing.

150116 Server Authentication Found (1)

150116 Server Authentication Found

archibus.vodacom.co.za/archibus

Finding #	14172492	**Severity**	Information Gathered - Level 1
Unique #	dffbf968-fa92-47b5-9380-8998cc37e2ba		
Group	Scan Diagnostics		
CWE	-	**Detection Date**	11 Feb 2024 21:02 GMT+0200
OWASP	-		
WASC	-		

Details

Threat
Server Authentication was found during the web application crawling.

Impact
N/A

Solution
N/A

Results

Server authentication found:
Url: https://archibus.vodacom.co.za/FPRWin/index.aspx
Type: unknown
Server authentication found:

Url: https://archibus.vodacom.co.za/FPRWin/index.aspx
Type: NTLM
Server authentication found:
Url: https://archibus.vodacom.co.za/FPRWin/
Type: unknown

150152 Forms Crawled (1)

150152 Forms Crawled

archibus.vodacom.co.za/archibus

Finding #	10510589	**Severity**	Information Gathered - Level 1
Unique #	2f2b8289-eae1-4614-b122-1a49fd3d8bc0		
Group	Scan Diagnostics		
CWE	-	**Detection Date**	11 Feb 2024 21:02 GMT+0200
OWASP	-		
WASC	-		

Details

Threat

The Results section lists the unique forms that were identified and submitted by the scanner. The forms listed in this QID do not include authentication forms (i.e. login forms), which are reported separately under QID 150115.

The scanner does a redundancy check on forms by inspecting the form fields. Forms determined to be the redundant based on identical form fields will not be tested. If desired, you can enable 'Include form action URI in form uniqueness calculation' in the WAS option profile to have the scanner also consider the form's action attribute in the redundancy check.

NOTE: Any regular expression specified under 'Redundant Links' are not applied to forms. Forms (unique or redundant) are not reported under QID 150140.

Impact

N/A

Solution

N/A

Results

Total internal forms seen (this count includes duplicate forms): 0

Crawled forms (Total: 0)
NOTE: This does not include authentication forms. Authentication forms are reported separately in QID 150115

150172 Requests Crawled (1)

150172 Requests Crawled

archibus.vodacom.co.za/archibus

Finding #	10510603	**Severity**	Information Gathered - Level 1
Unique #	6cae2eec-8347-4dd8-ad0b-b4733a6671ae		
Group	Scan Diagnostics		
CWE	-	**Detection Date**	11 Feb 2024 21:02 GMT+0200
OWASP	-		
WASC	-		

Details

Threat

WAS Web Application Report

The QID reports list of requests crawled by the Web application scanner appear in the Results section.

Impact
N/A

Solution
N/A

Results

Number of crawled XHRs (XHRs, Fetch and External XHRs): 97

Fetch Requests: 95
Method POST URI https://archibus.vodacom.co.za/Leasure-the-deed-will-the-clipt-Angely-ands-Banq?d=archibus.vodacom.co.za (Count: 95)

Number of External XHRs: 2

150247 Web Server and Technologies Detected (1)

150247 Web Server and Technologies Detected

archibus.vodacom.co.za/archibus

Finding #	14172491	**Severity**	Information Gathered - Level 1
Unique #	8ac4b422-4654-45fe-b7a8-4d00f7daae32		
Group	Scan Diagnostics		
CWE	CWE-200	**Detection Date**	11 Feb 2024 21:02 GMT+0200
OWASP	-		
WASC	-		

Details

Threat
Information disclosure is an application weakness in revealing sensitive data, such as technical details of the system or environment.

This check reports the various technologies used by the web application based on the information available in different components of the Request-Response.

Impact
An attacker may use sensitive data to exploit the target web application, its hosting network, or its users.

Solution
Ensure that your web servers do not reveal any sensitive information about your technology stack and system details

Please review the issues reported below:

Results

Number of technologies detected: 2
Technology name: Microsoft ASP.NET
Matched Components:
header match:
X-Powered-By:ASP.NET
Matched links: reporting only first 3 links
https://archibus.vodacom.co.za/FPRWin/
https://archibus.vodacom.co.za/FPRWin/index.aspx

Technology name: Microsoft IIS
Technology version: Microsoft IIS 10.0
Matched Components:
header match:

Server:Microsoft-IIS/10.0
Matched links: reporting only first 3 links
https://archibus.vodacom.co.za/FPRWin/
https://archibus.vodacom.co.za/FPRWin/index.aspx

150516 Web Application External URL Redirection (1)

150516 Web Application External URL Redirection — *archibus.vodacom.co.za/archibus*

Finding #	14172494	**Severity**	Information Gathered - Level 1
Unique #	7dbac962-c118-49bb-9972-6109bb7ab5c6		
Group	Scan Diagnostics		
CWE	-	**Detection Date**	11 Feb 2024 21:02 GMT+0200
OWASP	-		
WASC	-		

Details

Threat

External redirected links were discovered during the scan and are listed in the Results section.

Impact

Attackers can use external redirects without validation to redirect a user to a malicious URL. For example, if the trusted application is https://X.X.X.TrustQualys/test?url=qualys.com, the user is navigating to https://X.X.X.TrustQualys, and it is a trusted domain. However, there is an invalidated redirect, and the attacker can manipulate the redirection. The attacker can use this link https://X.X.X.TrustQualys/test?url=X.X.XReallyBadApp.com (for this example, ReallyBadApp is used, savvy malicious attackers will use more legitimate looking values) where the customer may be redirected to an external entity X.X.XReallyBadApp.com. This unintended redirect may lead to fishing or malware. Since the user was redirected from a trusted application, the user may be more willing to provide information.

Solution

As a standard avoid using external redirects and forwards in the application when possible. As a standard, avoid external redirects and forwards in the application when possible. Applications often are designed to redirect the user within the application and trusted external URLs. If a redirect parameter is used, ensure that the supplied value is valid and filtered based on trusted URLs. Setting up a whitelist would be most applicable to this technique. Reference: Unvalidated_Redirects_and_Forwards_Cheat_Sheet

Results

External Redirect URLs:
https://archibus.vodacom.co.za/archibus/ Redirects to
https://login.sso.vodacom.co.za/nidp/saml2/idpsend?id=archibus

https://archibus.vodacom.co.za/archibus/null Redirects to
https://login.sso.vodacom.co.za/nidp/saml2/idpsend?id=archibus

https://archibus.vodacom.co.za/archibus/null Redirects to
https://login.sso.vodacom.co.za/nidp/saml2/idpsend?id=archibus

150528 Server Returns HTTP 4XX Error Code During Scanning (1)

150528 Server Returns HTTP 4XX Error Code During Scanning — *archibus.vodacom.co.za/archibus*

Finding #	10510583	**Severity**	Information Gathered - Level 1
Unique #	35415709-818f-4b23-b1bc-8d2b39de1576		
Group	Scan Diagnostics		
CWE	-	**Detection Date**	11 Feb 2024 21:02 GMT+0200
OWASP	-		
WASC	-		

WAS Web Application Report

Details

Threat

During the WAS scan, links with HTTP 4xx response code were observed and these are listed in the Results section. The HTTP 4xx message indicates a client error. The list of supported 4xx response code are as below:

400 - Bad Request
401 - Unauthorized
403 - Forbidden
404 - Not Found
405 - Method Not Allowed
407 - Proxy Authentication Required
408 - Request Timeout
413 - Payload Too Large
414 - URI Too Long

Impact

The presence of a HTTP 4xx error during the crawl phase indicates that some problem exists on the website that will be encountered during normal usage of the Web application. Note WAS depends on responses to detect many vulnerabilities if the link does not respond with an expected response then any vulnerabilities present on such links may not be detected.

Solution

Review each link to determine why the client encountered an error while requesting the link. Additionally review and investigate the results of QID 150042 which lists 5xx errors, QID 150019 which lists unexpected response codes and QID 150097 which lists a potential blocked request.

Results

Number of links with 4xx response code: 45
(Only first 50 such links are listed)

401 https://archibus.vodacom.co.za/FPRWin/
401 https://archibus.vodacom.co.za/FPRWin/index.aspx
404 https://archibus.vodacom.co.za/_Incapsula_Resource?CWUDNSAI=23%22xinfo=10-107502277-0%200NNN%20RT%281686510550324%2012994%29%20q%280%20-1%20-1%200%29%20r%280%20-1%29%20B15%284%2c200%2c0%29%20U18%22incident_id=76900980359807166-515218109305526410%22edet=15%22cinfo=04000000%22rpinfo=0%22mth=GET
404 https://archibus.vodacom.co.za/_Incapsula_Resource?CWUDNSAI=23%22xinfo=10-112012598-0%200NNN%20RT%281691953444703%2013039%29%20q%280%20-1%20-1%204%29%20r%280%20-1%29%20B15%284%2c200%2c0%29%20U18%22incident_id=12800073032438640 3-54695758686847444 2%22edet=15%22cinfo=04000000%22rpinfo=0%22mth=GET
404 https://archibus.vodacom.co.za/_Incapsula_Resource?CWUDNSAI=23%22xinfo=11-128333115-0%200NNN%20RT%281686510547447%202871%29%20q%280%20-1%20-1%200%29%20r%280%20-1%29%20B15%284%2C200%2C0%29%20U18%22incident_id=76900980359807166-612085775202326667%22edet=15%22cinfo=04000000%22rpinfo=0%22mth=GET
404 https://archibus.vodacom.co.za/_Incapsula_Resource?CWUDNSAI=23%22xinfo=11-128333115-0%200NNN%20RT%281686510547447%202871%29%20q%280%20-1%20-1%200%29%20r%280%20-1%29%20B15%284%2c200%2c0%29%20U18%22incident_id=76900980359807166-61208577520232666 7%22edet=15%22cinfo=04000000%22rpinfo=0%22mth=GET
404 https://archibus.vodacom.co.za/_Incapsula_Resource?CWUDNSAI=23%22xinfo=11-74601801-0%200NNN%20RT%281694372516063%202785%29%20q%280%20-1%20-1%200%29%20r%280%20-1%29%20B15%284%2C200%2C0%29%20U18%22incident_id=76400410179907764-353379304890698315%22edet=15%22cinfo=04000000%22rpinfo=0%22mth=GET
404 https://archibus.vodacom.co.za/_Incapsula_Resource?CWUDNSAI=23%22xinfo=11-74601801-0%200NNN%20RT%281694372516063%202785%29%20q%280%20-1%20-1%200%29%20r%280%20-1%29%20B15%284%2c200%2c0%29%20U18%22incident_id=76400410179907764-35337930489069831 5%22edet=15%22cinfo=04000000%22rpinfo=0%22mth=GET
404 https://archibus.vodacom.co.za/_Incapsula_Resource?CWUDNSAI=23%22xinfo=12-140568936-0%200NNN%20RT%281699815739671%202292%29%20q%280%20-1%20-1%201%29%20r%280%20-1%29%20B15%284%2c200%2c0%29%20U18%22incident_id=76600119051698077 9-773471142739320268%22edet=15%22cinfo=04000000%22rpinfo=0%22mth=GET
404 https://archibus.vodacom.co.za/_Incapsula_Resource?CWUDNSAI=23%22xinfo=12-143394600-0%200NNN%20RT%281691953410996%20780%29%20q%280%20-1%20-1%200%29%20r%280%20-1%29%20B15%284%2c200%2c0%29%20U18%22incident_id=12800073032438640 3-68869439385449735 6%22edet=15%22cinfo=04000000%22rpinfo=0%22mth=GET
404 https://archibus.vodacom.co.za/_Incapsula_Resource?CWUDNSAI=23%22xinfo=13-133113832-0%200NNN%20RT%281699815739671%2015870%29%20q%280%20-1%20-1%200%29%20r%280%20-1%29%20B15%284%2c200%2c0%29%20U18%22incident_id=76600119051698077 9-728228691682663885%22edet=15%22cinfo=04000000%22rpinfo=0%22mth=GET
404 https://archibus.vodacom.co.za/_Incapsula_Resource?CWUDNSAI=23%22xinfo=13-50005422-0%200NNN%20RT%281684091004823%2015780%29%20q%280%20-1%20-1%201%29%20r%280%20-1%29%20B15%284%2c200%2c0%29%20U18%22incident_id=76800033012684013 8-244105402621364301%22edet=15%22cinfo=04000000%22rpinfo=0%22mth=GET
404 https://archibus.vodacom.co.za/_Incapsula_Resource?CWUDNSAI=23%22xinfo=13-51475396-0%200NNN%20RT%281696791744809%202625%29%20q%280%20-1%20-1%202%29%20r%280%20-1%29%20B15%284%2c200%2c0%29%20U18%22incident_id=76400046012960304 7-261986575540030349%22edet=15%22cinfo=04000000%22rpinfo=0%22mth=GET
404 https://archibus.vodacom.co.za/_Incapsula_Resource?CWUDNSAI=23%22xinfo=13-51475397-0%200NNN%20RT%281696791744809%2015891%29%20q%280%20-1%20-1%200%29%20r%280%20-1%29%20B15%284%2c200%2c0%29%20U18%22incident_id=76400046012960304 7-262001204198640525%22edet=15%22cinfo=04000000%22rpinfo=0%22mth=GET
404 https://archibus.vodacom.co.za/_Incapsula_Resource?CWUDNSAI=23%22xinfo=14-56552041-0%200NNN%20RT%281684091004822%202271%29%20q%280%20-1%20-1%200%29%20r%280%20-1%29%20B15%284%2c200%2c0%29%20U18%22incident_id=76800033012684013 8-290605261188499534%22edet=15%22cinfo=04000000%22rpinfo=0%22mth=GET
404 https://archibus.vodacom.co.za/_Incapsula_Resource?CWUDNSAI=23%22xinfo=36-7073891-0%200NNN%20RT%281705258999531%202780%29%20q%280%20-1%20-1%200%29%20r%280%20-1%29%20B15%284%2c200%2c0%29%20U18%22incident_id=16880000503220873 14-449426280902823 40%22edet=15%22cinfo=04000000%22rpinfo=0%22mth=GET
404 https://archibus.vodacom.co.za/_Incapsula_Resource?CWUDNSAI=23%22xinfo=37-6345043-0%200NNN%20RT%281705258999533%2016038%29%20q%280%20-1%20-1%200%29%20r%280%20-1%29%20B15%284%2c200%2c0%29%20U18%22incident_id=16880000503220873 14-407389717989953 01%22edet=15%22cinfo=04000000%22rpinfo=0%22mth=GET
404 https://archibus.vodacom.co.za/_Incapsula_Resource?CWUDNSAI=23%22xinfo=4-9346511-0%200NNN%20RT%281694372516064%2015875%29%20q%280%20-1%20-1%200%29%20r%280%20-1%29%20B15%284%2c200%2c0%29%20U18%22incident_id=76400041017990776 4-456022061573760 68%22edet=15%22cinfo=04000000%22rpinfo=0%22mth=GET
404 https://archibus.vodacom.co.za/_Incapsula_Resource?CWUDNSAI=23%22xinfo=5-218372829-0%200NNN%20RT%281688929454117%202786%29%20q%280%20-1%20-1%201%29%20r%280%20-1%29%20B15%284%2c200%2c0%29%20U18%22incident_id=44900158057159480 0-111895544297063411 7%22edet=15%22cinfo=04000000%22rpinfo=0%22mth=GET
404 https://archibus.vodacom.co.za/_Incapsula_Resource?CWUDNSAI=23%22xinfo=5-85633350-0%200NNN%20RT%281702234935613%208793%29%20q%280%20-1%20-1%200%29%20r%280%20-1%29%20B15%284%2c200%2c0%29%20U18%22incident_id=77000117043697588 7-430458772260003141%22edet=15%22cinfo=04000000%22rpinfo=0%22mth=GET
404 https://archibus.vodacom.co.za/_Incapsula_Resource?CWUDNSAI=23%22xinfo=6-50761907-0%200NNN%20RT%281691953429171%2013568%29%20q%280%20-1%20-1%200%29%20r%280%20-1%29%20B15%284%2c200%2c0%29%20U18%22incident_id=12800073032438640 3-257296789038699078%22edet=15%22cinfo=04000000%22rpinfo=0%22mth=GET
404 https://archibus.vodacom.co.za/_Incapsula_Resource?CWUDNSAI=23%22xinfo=7-120841302-0%200NNN%20RT%281688929454119%2016073%29%20q%280%20-1%20-1%200%29%20r

%280%20-1%29%20B15%284%2c200%2c0%29%20U18%22incident_id=449001580571594800-631738012224530311%22edet=15%22cinfo=04000000%22rpinfo=0%22mth=GET
404 https://archibus.vodacom.co.za/_Incapsula_Resource?CWUDNSAI=23%22xinfo=7-74746777-0%200NNN%20RT%281702234928535%202882%29%20q%280%20-1%20-1%200%29%20r
%280%20-1%29%20B15%284%2c200%2c0%29%20U18%22incident_id=770001170436975887-376282892306881863%22edet=15%22cinfo=04000000%22rpinfo=0%22mth=GET
404 https://archibus.vodacom.co.za/_Incapsula_Resource?CWUDNSAI=23%22xinfo=8-71777546-0%200NNN%20RT%281691953415895%209146%29%20q%280%20-1%20-1%202%29%20r
%280%20-1%29%20B15%284%2c200%2c0%29%20U18%22incident_id=128000730324386403-355359155923456584%22edet=15%22cinfo=04000000%22rpinfo=0%22mth=GET
404 https://archibus.vodacom.co.za/docs/
404 https://archibus.vodacom.co.za/docs/RELEASE-NOTES.txt
404 https://archibus.vodacom.co.za/docs/api/
404 https://archibus.vodacom.co.za/docs/api/index.html
404 https://archibus.vodacom.co.za/docs/appdev/
404 https://archibus.vodacom.co.za/docs/changelog.html
404 https://archibus.vodacom.co.za/docs/cluster-howto.html
404 https://archibus.vodacom.co.za/docs/config/
404 https://archibus.vodacom.co.za/docs/deployer-howto.html
404 https://archibus.vodacom.co.za/docs/jndi-datasource-examples-howto.html
404 https://archibus.vodacom.co.za/docs/manager-howto.html
404 https://archibus.vodacom.co.za/docs/realm-howto.html
404 https://archibus.vodacom.co.za/docs/security-howto.html
404 https://archibus.vodacom.co.za/docs/setup.html
404 https://archibus.vodacom.co.za/examples/
404 https://archibus.vodacom.co.za/host-manager/
404 https://archibus.vodacom.co.za/host-manager/html
404 https://archibus.vodacom.co.za/manager/
404 https://archibus.vodacom.co.za/manager/html
404 https://archibus.vodacom.co.za/manager/status
404 https://archibus.vodacom.co.za/null

150546 First Link Crawled Response Code Information (1)

150546 First Link Crawled Response Code Information

archibus.vodacom.co.za/archibus

Finding #	10510593	**Severity**	Information Gathered - Level 1
Unique #	0a78b347-3fc1-4921-97ad-a4fd9ca4133b		
Group	Scan Diagnostics		
CWE	-	**Detection Date**	11 Feb 2024 21:02 GMT+0200
OWASP	-		
WASC	-		

Details

Threat

The Web server returned the following information from where the Web application scanning engine initiated. Information reported includes First Link Crawled, response Code, response Header, and response Body (first 500 characters). The first link crawled is the "Web Application URL (or Swagger file URL)" set in the Web Application profile.

Impact

An erroneous response might be indicative of a problem in the Web server, or the scan configuration.

Solution

Review the information to check if this is in line with the expected scan configuration. Refer to the output of QIDs 150009, 150019, 150021, 150042 and 150528 (if present) for additional details.

Results

Base URI: https://archibus.vodacom.co.za/archibus/
Response Code: 302
Response Header:
content-length: 0
content-security-policy-report-only: default-src 'self' 'unsafe-eval' 'unsafe-hashes' 'unsafe-inline' data: blob: ; form-action 'none' data: blob: ; report-uri /csp_report
location: https://login.sso.vodacom.co.za/nidp/saml2/idpsend?id=archibus
server: BigIP
x-cdn: Imperva
x-iinfo: 60-17038774-17038780 PNNy RT(1707678198155 3619) q(0 0 0 0) r(2 2) U11
Set-Cookie: visid_incap_2776849=2mCPlvHbTaSKgOs2WBZQC/YZyWUAAAAAQUIPAAAAAAAWwMvjPe13zMYdphiXlTQy; HttpOnly; expires=Sun, 09-Feb-2025 22:21:11 GMT; domain=.vodacom.co.za; path=/
Set-Cookie: nlbi_2776849=ogi1WuqyhRkuEuYJZU49BAAAAABLcyLrdKjEmQdibbXYNFmh; domain=.vodacom.co.za; path=/
Set-Cookie: incap_ses_1687_2776849=9uxXXci+jlSe7PgfvG1pF/YZyWUAAAAAfr+BmEPjvWAiYHFjqA+aDQ==; domain=.vodacom.co.za; path=/

Response Body:
<html><head></head><body></body></html>

150621 List of JavaScript Links (1)

150621 List of JavaScript Links — *archibus.vodacom.co.za/archibus*

Finding #	10510605	**Severity**	Information Gathered - Level 1
Unique #	00bfc91f-16c4-4d7c-8da2-f471f57ba8a1		
Group	Scan Diagnostics		
CWE	-	**Detection Date**	11 Feb 2024 21:02 GMT+0200
OWASP	-		
WASC	-		

Details

Threat
This QID reports all the JavaScript links that are in-scope of this scan.

Impact
JavaScript links may pose security risks such as XSS, CSRF.

Solution
Verify JavaScript links are intentional and required for your web application.
Review any third party scripts that are hosted on your local server instead of using CDN.
Update all the JavaScript libraries with latest version as applicable.

Results

JavaScript Links were found while crawling.
Total Number of Links: 32
https://archibus.vodacom.co.za/Leasure-the-deed-will-the-clipt-Angely-ands-Banq
https://archibus.vodacom.co.za/_Incapsula_Resource?SWJIYLWA=719d34d31c8e3a6e6fffd425f7e032f3&ns=19&cb=1246563959
https://archibus.vodacom.co.za/_Incapsula_Resource?SWJIYLWA=719d34d31c8e3a6e6fffd425f7e032f3&ns=5&cb=2085785877
https://archibus.vodacom.co.za/_Incapsula_Resource?SWJIYLWA=719d34d31c8e3a6e6fffd425f7e032f3%22ns=10%22cb=718590515
https://archibus.vodacom.co.za/Leasure-the-deed-will-the-clipt-Angely-ands-Banq?d=archibus.vodacom.co.za
https://archibus.vodacom.co.za/_Incapsula_Resource?SWJIYLWA=719d34d31c8e3a6e6fffd425f7e032f3&ns=10&cb=718590515
https://archibus.vodacom.co.za/_Incapsula_Resource?SWJIYLWA=719d34d31c8e3a6e6fffd425f7e032f3&ns=30&cb=757409821
https://archibus.vodacom.co.za/_Incapsula_Resource?SWJIYLWA=719d34d31c8e3a6e6fffd425f7e032f3%22ns=23%22cb=682184485
https://archibus.vodacom.co.za/_Incapsula_Resource?SWJIYLWA=719d34d31c8e3a6e6fffd425f7e032f3&ns=23&cb=682184485
https://archibus.vodacom.co.za/_Incapsula_Resource?SWJIYLWA=719d34d31c8e3a6e6fffd425f7e032f3&ns=49&cb=1264811833
https://archibus.vodacom.co.za/_Incapsula_Resource?SWJIYLWA=719d34d31c8e3a6e6fffd425f7e032f3&ns=52&cb=1058230007
https://archibus.vodacom.co.za/_Incapsula_Resource?SWJIYLWA=719d34d31c8e3a6e6fffd425f7e032f3&ns=31&cb=292274561
https://archibus.vodacom.co.za/_Incapsula_Resource?SWJIYLWA=719d34d31c8e3a6e6fffd425f7e032f3%22ns=31%22cb=292274561
https://archibus.vodacom.co.za/_Incapsula_Resource?SWJIYLWA=719d34d31c8e3a6e6fffd425f7e032f3%22ns=33%22cb=462486625
https://archibus.vodacom.co.za/_Incapsula_Resource?SWJIYLWA=719d34d31c8e3a6e6fffd425f7e032f3%22ns=40%22cb=1925770764
https://archibus.vodacom.co.za/_Incapsula_Resource?SWJIYLWA=719d34d31c8e3a6e6fffd425f7e032f3%22ns=57%22cb=149715920
https://archibus.vodacom.co.za/_Incapsula_Resource?SWJIYLWA=719d34d31c8e3a6e6fffd425f7e032f3%22ns=62%22cb=759071798
https://archibus.vodacom.co.za/_Incapsula_Resource?SWJIYLWA=719d34d31c8e3a6e6fffd425f7e032f3%22ns=63%22cb=261016948
https://archibus.vodacom.co.za/_Incapsula_Resource?SWJIYLWA=719d34d31c8e3a6e6fffd425f7e032f3&ns=33&cb=462486625
https://archibus.vodacom.co.za/_Incapsula_Resource?SWJIYLWA=719d34d31c8e3a6e6fffd425f7e032f3&ns=40&cb=1925770764
https://archibus.vodacom.co.za/_Incapsula_Resource?SWJIYLWA=719d34d31c8e3a6e6fffd425f7e032f3&ns=57&cb=149715920
https://archibus.vodacom.co.za/_Incapsula_Resource?SWJIYLWA=719d34d31c8e3a6e6fffd425f7e032f3&ns=63&cb=261016948
https://archibus.vodacom.co.za/_Incapsula_Resource?SWJIYLWA=719d34d31c8e3a6e6fffd425f7e032f3&ns=79&cb=83869883
https://archibus.vodacom.co.za/_Incapsula_Resource?SWJIYLWA=719d34d31c8e3a6e6fffd425f7e032f3&ns=62&cb=759071798
https://archibus.vodacom.co.za/_Incapsula_Resource?SWJIYLWA=719d34d31c8e3a6e6fffd425f7e032f3&ns=78&cb=352187491
https://archibus.vodacom.co.za/_Incapsula_Resource?SWJIYLWA=719d34d31c8e3a6e6fffd425f7e032f3%22ns=88%22cb=1925157912
https://archibus.vodacom.co.za/_Incapsula_Resource?SWJIYLWA=719d34d31c8e3a6e6fffd425f7e032f3%22ns=78%22cb=352187491
https://archibus.vodacom.co.za/_Incapsula_Resource?SWJIYLWA=719d34d31c8e3a6e6fffd425f7e032f3&ns=88&cb=1925157912
https://archibus.vodacom.co.za/_Incapsula_Resource?SWJIYLWA=719d34d31c8e3a6e6fffd425f7e032f3%22ns=98%22cb=1649221342
https://archibus.vodacom.co.za/_Incapsula_Resource?SWJIYLWA=719d34d31c8e3a6e6fffd425f7e032f3%22ns=87%22cb=669575803
https://archibus.vodacom.co.za/_Incapsula_Resource?SWJIYLWA=719d34d31c8e3a6e6fffd425f7e032f3&ns=87&cb=669575803
https://archibus.vodacom.co.za/_Incapsula_Resource?SWJIYLWA=719d34d31c8e3a6e6fffd425f7e032f3&ns=98&cb=1649221342

38116 SSL Server Information Retrieval (1)

WAS Web Application Report

38116 SSL Server Information Retrieval

archibus.vodacom.co.za/archibus

Finding #	10510615	**Severity**	Information Gathered - Level 1
Unique #	378be5c9-02fd-4c12-9537-157c5a6ab5e0		
Group	Scan Diagnostics		
CWE	-	**Detection Date**	11 Feb 2024 21:02 GMT+0200
OWASP	-		
WASC	-		

Details

Threat

The following is a list of supported SSL ciphers.

Note: If a cipher is included in this list it means that it was possible to establish a SSL connection using that cipher. There are some web servers setups that allow connections to be established using a LOW grade cipher, only to provide a web page stating that the URL is accessible only through a non-LOW grade cipher. In this case even though LOW grade cipher will be listed here QID 38140 will not be reported.

Impact

N/A

Solution

N/A

SSL Data

Flags	-
Protocol	tcp
Virtual Host	45.223.138.96
IP	45.223.138.96
Port	443
Result	#table cols="6" CIPHER KEY-EXCHANGE AUTHENTICATION MAC ENCRYPTION(KEY-STRENGTH) GRADE SSLv2_PROTOCOL_IS_DISABLED _ _ _ _ _ SSLv3_PROTOCOL_IS_DISABLED _ _ _ _ _ TLSv1_PROTOCOL_IS_DISABLED _ _ _ _ _ TLSv1.1_PROTOCOL_IS_DISABLED _ _ _ _ _ TLSv1.2_PROTOCOL_IS_ENABLED _ _ _ _ _ TLSv1.2 COMPRESSION_METHOD None _ _ _ AES128-SHA RSA RSA SHA1 AES(128) MEDIUM AES256-SH RSA RSA SHA1 AES(256) HIGH CAMELLIA128-SHA RSA RSA SHA1 Camellia(128) MEDIUM CAMELLIA256-SHA RSA RSA SHA1 Camellia(256) HIGH AES1 GCM-SHA256 RSA RSA AEAD AESGCM(128) MEDIUM AES256-GCM-SHA384 RSA RSA AEAD AESGCM(256) HIGH ECDHE-RSA-AES128-SHA ECDH RSA SHA1 AES(128) MEDIUM ECDHE-RSA-AES256-SHA ECDH RSA SHA1 AES(256) HIGH ECDHE-RSA-AES128-SHA256 ECDH RSA SHA256 AES(128) MEDI ECDHE-RSA-AES256-SHA384 ECDH RSA SHA384 AES(256) HIGH ECDHE-RSA-AES128-GCM-SHA256 ECDH RSA AEAD AESGCM(128) MEDIUM ECDHE RSA-AES256-GCM-SHA384 ECDH RSA AEAD AESGCM(256) HIGH ECDHE-RSA-CHACHA20-POLY1305 ECDH RSA AEAD CHACHA20/POLY1305(256) HI AES128-SHA256 RSA RSA SHA256 AES(128) MEDIUM AES256-SHA256 RSA RSA SHA256 AES(256) HIGH TLSv1.3_PROTOCOL_IS_ENABLED _ _ _ _ _ TLS13-AES-128-GCM-SHA256 N/A N/A AEAD AESGCM(128) MEDIUM TLS13-AES-256-GCM-SHA384 N/A N/A AEAD AESGCM(256) HIGH TLS13-CHACHA2 POLY1305-SHA256 N/A N/A AEAD CHACHA20/POLY1305(256) HIGH

Info List

Info #1

Ciphers

Name	Auth	Encryption	Grade	Key Exchange	Mac	Protocol
TLS13-AES-128-GCM-SHA256	N/A	AESGCM(128)	MEDIUM	N/A	AEAD	TLSv1.3
TLS13-AES-128-GCM-SHA256	N/A	AESGCM(256)	HIGH	N/A	AEAD	TLSv1.3
TLS13-AES-128-GCM-SHA256	N/A	CHACHA20/POLY1305(256)	HIGH	N/A	AEAD	TLSv1.3

38291 SSL Session Caching Information (1)

38291 SSL Session Caching Information

archibus.vodacom.co.za/archibus

Finding #	10510609	**Severity**	Information Gathered - Level 1
Unique #	3121b915-641d-45c0-8360-e49dd8b86ae0		
Group	Scan Diagnostics		
CWE	-	**Detection Date**	11 Feb 2024 21:02 GMT+0200
OWASP	-		
WASC	-		

Details

Threat

SSL session is a collection of security parameters that are negotiated by the SSL client and server for each SSL connection. SSL session caching is targeted to reduce the overhead of negotiations in recurring SSL connections. SSL sessions can be reused to resume an earlier connection or to establish multiple simultaneous connections. The client suggests an SSL session to be reused by identifying the session with a Session-ID during SSL handshake. If the server finds it appropriate to reuse the session, then they both proceed to secure communication with already known security parameters.

This test determines if SSL session caching is enabled on the host.

Impact

SSL session caching is part of the SSL and TLS protocols and is not a security threat. The result of this test is for informational purposes only.

Solution

N/A

SSL Data

Flags	-
Protocol	tcp
Virtual Host	45.223.138.96
IP	45.223.138.96
Port	443
Result	TLSv1.2 session caching is enabled on the target. TLSv1.3 session caching is enabled on the target.

Info List

WAS Web Application Report

Info #1

38597 Secure Sockets Layer/Transport Layer Security (SSL/TLS) Invalid Protocol Version Tolerance (1)

38597 Secure Sockets Layer/Transport Layer Security (SSL/TLS) Invalid Protocol Version Tolerance

archibus.vodacom.co.za/archibus

Finding #	10510614	**Severity**	Information Gathered - Level 1
Unique #	77427923-7034-45c0-8875-ec7aaed13424		
Group	Scan Diagnostics		
CWE	-	**Detection Date**	11 Feb 2024 21:02 GMT+0200
OWASP	-		
WASC	-		

Details

Threat

SSL/TLS protocols have different version that can be supported by both the client and the server. This test attempts to send invalid protocol versions to the target in order to find out what is the target's behavior. The results section contains a table that indicates what was the target's response to each of our tests.

Impact

N/A

Solution

N/A

SSL Data

Flags	-
Protocol	tcp
Virtual Host	45.223.138.96
IP	45.223.138.96
Port	443
Result	#table cols=2 my_version target_version 0304 0303 0399 0303 0400 0303 0499 0303

Info List

Info #1

38600 SSL Certificate will expire within next six months (1)

38600 SSL Certificate will expire within next six months

archibus.vodacom.co.za/archibus

Finding #	10510608	**Severity**	Information Gathered - Level 1
Unique #	8177a8a8-1404-4689-860d-251a77557e89		
Group	Scan Diagnostics		
CWE	-	**Detection Date**	11 Feb 2024 21:02 GMT+0200
OWASP	-		
WASC	-		

Details

Threat
Certificates are used for authentication purposes in different protocols such as SSL/TLS. Each certificate has a validity period outside of which it is supposed to be considered invalid. This QID is reported to inform that a certificate will expire within next six months. The advance notice can be helpful since obtaining a certificate can take some time.

Impact
Expired certificates can cause connection disruptions or compromise the integrity and privacy of the connections being protected by the certificates.

Solution
Contact the certificate authority that signed your certificate to arrange for a renewal.

SSL Data

Flags	-
Protocol	tcp
Virtual Host	45.223.138.96
IP	45.223.138.96
Port	443
Result	Certificate #0 CN=imperva.com The certificate will expire within six months: Jul 16 13:49:41 2024 GMT

Info List

Info #1

Certificate Fingerprint:5838E53F3C592C3FE144A59A3FF1EB4125C036D90CAEA8406E97249764E16408

38704 Secure Sockets Layer/Transport Layer Security (SSL/TLS) Key Exchange Methods (1)

38704 Secure Sockets Layer/Transport Layer Security (SSL/TLS) Key Exchange Methods

archibus.vodacom.co.za/archibus

Finding #	10510616	**Severity**	Information Gathered - Level 1
Unique #	bd28e71e-4df1-4860-8882-64f90e1902d4		
Group	Scan Diagnostics		
CWE	-	**Detection Date**	11 Feb 2024 21:02 GMT+0200
OWASP	-		
WASC	-		

Details

Threat
The following is a list of SSL/TLS key exchange methods supported by the server, along with their respective key sizes, strengths and ciphers.

Impact
N/A

Solution
N/A

SSL Data

Flags	-
Protocol	tcp
Virtual Host	45.223.138.96
IP	45.223.138.96
Port	443
Result	#table cols="6" NAME GROUP KEY-SIZE FORWARD-SECRET CLASSICAL-STRENGTH QUANTUM-STRENGTH TLSv1.2 _ _ _ _ _ RSA _ 2048 no 110 low ECDHE x25519 256 yes 128 low ECDHE secp256r1 256 yes 128 low ECDHE x448 448 yes 224 low ECDHE secp521r1 521 yes 260 low ECDHE secp384r1 384 yes 192 low TLSv1.3 _ _ _ _ _ ECDHE x25519 256 yes 128 low ECDHE secp256r1 256 yes 128 low ECDHE x448 448 yes 224 low ECDHE secp521r1 521 yes low ECDHE secp384r1 384 yes 192 low

Info List

Info #1

Kexs

Kex	Group	Protocol	Key Size		Classical	Quantum
RSA		TLSv1.2	2048	no	110	low
ECDHE		TLSv1.2	256	yes	128	low
ECDHE		TLSv1.2	256	yes	128	low
ECDHE		TLSv1.2	448	yes	224	low
ECDHE		TLSv1.2	521	yes	260	low
ECDHE		TLSv1.2	384	yes	192	low
ECDHE		TLSv1.3	256	yes	128	low
ECDHE		TLSv1.3	256	yes	128	low
ECDHE		TLSv1.3	448	yes	224	low
ECDHE		TLSv1.3	521	yes	260	low
ECDHE		TLSv1.3	384	yes	192	low

38706 Secure Sockets Layer/Transport Layer Security (SSL/TLS) Protocol Properties (1)

38706 Secure Sockets Layer/Transport Layer Security (SSL/TLS) Protocol Properties

archibus.vodacom.co.za/archibus

Finding #	10510617	**Severity**	Information Gathered - Level 1
Unique #	88056f92-0571-49ff-a145-f53f795c3db6		
Group	Scan Diagnostics		
CWE	-	**Detection Date**	11 Feb 2024 21:02 GMT+0200
OWASP	-		
WASC	-		

Details

Threat

The following is a list of detected SSL/TLS protocol properties.

Impact

Items include:

- Extended Master Secret: indicates whether the extended_master_secret extension is supported or required by the server. This extension enhances security and is recommended. Applicable to TLSv1, TLSv1.1, TLSv1.2, DTLSv1, DTLSv1.2
- Encrypt Then MAC: indicates whether the encrypt_then_mac extension is supported or required by the server. This extension enhances the security of non-AEAD ciphers and is recommended. Applicable to TLSv1, TLSv1.1, TLSv1.2, DTLSv1, DTLSv1.2
- Heartbeat: indicates whether the heartbeat extension is supported. It is not recommended to enable this, except for DTLS. Applicable to TLSv1, TLSv1.1, TLSv1.2, TLSv1.3, DTLSv1, DTLSv1.2
- Truncated HMAC: indicates whether the truncated_hmac extension is supported. This can degrade security and is not recommended. Applicable to TLSv1, TLSv1.1, TLSv1.2, DTLSv1, DTLSv1.2
- Cipher priority: indicates whether client, server or both determine the priority of ciphers. Having the server determine the priority is recommended. Applicable to SSLv3, TLSv1, TLSv1.1, TLSv1.2, TLSv1.3, DTLSv1, DTLSv1.2

Solution

N/A

SSL Data

Flags	-
Protocol	tcp
Virtual Host	45.223.138.96
IP	45.223.138.96
Port	443
Result	#table cols="2" NAME STATUS TLSv1.2 _ Extended_Master_Secret yes Encrypt_Then_MAC yes Heartbeat no Truncated_HMAC no Cipher_priority_controlled_ server OCSP_stapling no SCT_extension no TLSv1.3 _ Heartbeat no Cipher_priority_controlled_by server OCSP_stapling no SCT_extension no

Info List

Info #1

Props

Name	Value	Protocol
Extended Master Secret	yes	TLSv1.2
Encrypt Then MAC	yes	TLSv1.2
Heartbeat	no	TLSv1.2
Truncated HMAC	no	TLSv1.2
Cipher priority controlled by	server	TLSv1.2
OCSP stapling	no	TLSv1.2
SCT extension	no	TLSv1.2
Heartbeat	no	TLSv1.3
Cipher priority controlled by	server	TLSv1.3
OCSP stapling	no	TLSv1.3
SCT extension	no	TLSv1.3

38717 Secure Sockets Layer (SSL) Certificate Online Certificate Status Protocol (OCSP) Information (1)

38717 Secure Sockets Layer (SSL) Certificate Online Certificate Status Protocol (OCSP) Information

archibus.vodacom.co.za/archibus

Finding #	10510610	**Severity**	Information Gathered - Level 1
Unique #	8a7bd7af-55b1-4e90-b633-de62a15e292d		
Group	Scan Diagnostics		
CWE	-	**Detection Date**	11 Feb 2024 21:02 GMT+0200
OWASP	-		
WASC	-		

Details

Threat

OCSP (Online Certificate Status Protocol) is a protocol to determine the status of an SSL certificate, specifically whether a certificate has been revoked by the issuing certificate authority. SSL servers can provide the OCSP status of their certificate as part of the SSL/TLS handshake. This information is referred to as "Status Request" or "OCSP Stapling".

Impact

N/A

Solution

N/A

SSL Data

Flags	-
Protocol	tcp
Virtual Host	45.223.138.96
IP	45.223.138.96
Port	443
Result	Certificate #0 CN=archibus.vodacom.co.za,O=Vodafone_Group_Services_Limited,L=Newbury,C=GB OCSP status: good

Info List

Info #1

Certificate Fingerprint:0240E35B84FE2BCC96395D0CE97B03D511E35FC83F24034E9B73A3E054FA3A32

38718 Secure Sockets Layer (SSL) Certificate Transparency Information (1)

38718 Secure Sockets Layer (SSL) Certificate Transparency Information *archibus.vodacom.co.za/archibus*

Finding #	10510611	**Severity**	Information Gathered - Level 1
Unique #	7386bca5-2111-4796-b509-a354873e3df5		
Group	Scan Diagnostics		
CWE	-	**Detection Date**	11 Feb 2024 21:02 GMT+0200
OWASP	-		
WASC	-		

Details

Threat

SSL Certificate Transparency is an industry effort to improve visibility into the process of how certificate authorities issue certificates. It is designed to allow the owners of domain names to find all certificates that have been issued for their domains, and which certificate authorities have issued them. This is done by requiring certificate authorities to publish all issued certificates in public logs. TLS servers can then provide cryptographic evidence to TLS clients that the server certificate has been registered in public logs, thus providing some degree of confidence that the certificate is legitimate. Such cryptographic evidence is referred to as an "SCT Log Proof".

The information below lists all validated SCT Log Proofs for server certificates along with information about the public log, where available.

Impact

N/A

Solution

N/A

SSL Data

Flags	-
Protocol	tcp
Virtual Host	45.223.138.96
IP	45.223.138.96
Port	443
Result	#table cols="6" Source Validated Name URL ID Time Certificate_#0 _ CN=archibus.vodacom.co.za,O=Vodafone_Group_Services_Limited,L=Newbury,C=GB _ _

Certificate no (unknown) (unknown) eecdd064d5db1acec55cb79db4cd13a23287467cbcecdec351485946711fb59b Thu_01_Jan_1970_12:00:00_AM_GMT Certificate no (unknown) (unknown) 48b0e36bdaa647340fe56a02fa9d30eb1c5201cb56dd2c81d9bbbfab39d88473 Thu_01_Jan_1970_12:00:00_AM_GMT Certificate no (unknown) (unknown) dab6bf6b3fb5b6229f9bc2bb5c6be87091716cbb51848534bda43d3048d7fbab Thu_01_Jan_1970_12:00:00_AM_GMT Certificate_#0 _ CN=imperva.com _ _ _ Certificate no (unknown) (unknown) 76ff883f0ab6fb9551c261ccf587ba34b4a4cdbb29dc68420a9fe6674c5a3a74 Thu_01_Jan_1970_12:00:00_AM_GMT Certificate no (unknown) (unknown) 3b5377753e2db9804e8b305b06fe403b67d84fc3f4c7bd000d2d726fe1fad417 Thu_01_Jan_1970_12:00:00_AM_GMT Certificate no (unknown) (unknown) 48b0e36bdaa647340fe56a02fa9d30eb1c5201cb56dd2c81d9bbbfab39d88473 Thu_01_Jan_1970_12:00:00_AM_GMT

Info List

Info #1

Certificate Fingerprint:5838E53F3C592C3FE144A59A3FF1EB4125C036D90CAEA8406E97249764E16408

42350 TLS Secure Renegotiation Extension Support Information (1)

42350 TLS Secure Renegotiation Extension Support Information

archibus.vodacom.co.za/archibus

Finding #	10510613	**Severity**	Information Gathered - Level 1
Unique #	899a7e26-ab72-4bec-b725-329f4aa9e43f		
Group	Scan Diagnostics		
CWE	-	**Detection Date**	11 Feb 2024 21:02 GMT+0200
OWASP	-		
WASC	-		

Details

Threat

Secure Socket Layer (SSL) and Transport Layer Security (TLS) renegotiation are vulnerable to an attack in which the attacker forms a TLS connection with the target server, injects content of his choice, and then splices in a new TLS connection from a client. The server treats the client's initial TLS handshake as a renegotiation and thus believes that the initial data transmitted by the attacker is from the same entity as the subsequent client data. TLS protocol was extended to cryptographically tierenegotiations to the TLS connections they are being performed over. This is referred to as TLS secure renegotiation extension. This detection determines whether the TLS secure renegotiation extension is supported by the server or not.

Impact

N/A

Solution

N/A

SSL Data

Flags	-
Protocol	tcp
Virtual Host	45.223.138.96
IP	45.223.138.96
Port	443
Result	TLS Secure Renegotiation Extension Status: supported.

Info List

Info #1

WAS Web Application Report

45038 Host Scan Time - Scanner (1)

45038 Host Scan Time - Scanner

archibus.vodacom.co.za/archibus

Finding #	10510592	**Severity**	Information Gathered - Level 1
Unique #	d1314843-9e2a-4a7f-8b7e-b32e33503d3b		
Group	Scan Diagnostics		
CWE	-	**Detection Date**	11 Feb 2024 21:02 GMT+0200
OWASP	-		
WASC	-		

Details

Threat

The Host Scan Time is the period of time it takes the scanning engine to perform the vulnerability assessment of a single target host. The Host Scan Time for this host is reported in the Result section below.

The Host Scan Time does not have a direct correlation to the Duration time as displayed in the Report Summary section of a scan results report. The Duration is the period of time it takes the service to perform a scan task. The Duration includes the time it takes the service to scan all hosts, which may involve parallel scanning. It also includes the time it takes for a scanner appliance to pick up the scan task and transfer the results back to the service's Secure Operating Center. Further, when a scan task is distributed across multiple scanners, the Duration includes the time it takes to perform parallel host scanning on all scanners.

Impact

N/A

Solution

N/A

SSL Data

Flags	-
Protocol	-
Virtual Host	archibus.vodacom.co.za
IP	45.223.138.96
Port	-
Result	Scan duration: 5157 seconds Start time: Sun Feb 11 19:02:08 UTC 2024 End time: Sun Feb 11 20:28:05 UTC 2024

Info List

Info #1

6 DNS Host Name (1)

6 DNS Host Name

archibus.vodacom.co.za/archibus

Finding #	10510606	**Severity**	Information Gathered - Level 1
Unique #	ffa613a0-5130-45df-bda5-36cdf36e9af7		
Group	Scan Diagnostics		
CWE	-	**Detection Date**	11 Feb 2024 21:02 GMT+0200
OWASP	-		
WASC	-		

Details

Threat
The fully qualified domain name of this host, if it was obtained from a DNS server, is displayed in the RESULT section.

Impact
N/A

Solution
N/A

SSL Data

Flags	-
Protocol	-
Virtual Host	45.223.138.96
IP	45.223.138.96
Port	-
Result	#table IP_address Host_name 45.223.138.96 No_registered_hostname

Info List

Info #1

86002 SSL Certificate - Information (1)

86002 SSL Certificate - Information *archibus.vodacom.co.za/archibus*

Finding #	10510607	**Severity**	Information Gathered - Level 1
Unique #	6b1fa8ed-a6c4-4545-be3b-7b77ad5e01f6		
Group	Scan Diagnostics		
CWE	-	**Detection Date**	11 Feb 2024 21:02 GMT+0200
OWASP	-		
WASC	-		

Details

Threat
SSL certificate information is provided in the Results section.

Impact
N/A

Solution
N/A

SSL Data

Flags	-

WAS Web Application Report

Protocol	tcp
Virtual Host	45.223.138.96
IP	45.223.138.96
Port	443
Result	#table cols="2" NAME VALUE (0)CERTIFICATE_0 _ (0)Version 3_(0x2) (0)Serial_Number _05:c6:21:a0:8b:cb:9d:a5:a9:50:27:34:56:03:00:0f_ (0)Signature_Algorithm sha256WithRSAEncryption (0)ISSUER_NAME _ countryName US _organizationName DigiCert_Inc _commonName DigiCert_SHA2_Secure_Server_CA (0)SUBJECT_NAME _ countryName GB _localityName Newbury _organizationName Vodafone_Group_Services_Limited _commonName archibus.vodacom.co.za (0)Valid_From Aug_11_00:00:00_2023_GMT (0)Valid_Till Aug_13_23:59:59_2024_GMT (0)Public_Key_Algorithm rsaEncryption (0)RSA_Public_Key (2048_bit) (0) _RSA_Public-Key:_(2048_bit) (0) _Modulus: (0) _00:95:50:81:28:a9:f1:89:02:18:87:b2:cb:e9:6f: (0) _6d:73:ee:e6 92:08:28:0b:71:fc:d7:01:34:86: (0) _43:c0:9c:74:c4:23:a9:cc:ef:d1:8d:61:25:27:3d: (0) _9f:f0:8b:65:be:57:1e:76:2e:e0:75:ca:9b:b1:8e: (0) _11:b5:5c:8b: 58:07:77:d1:15:e3:fc:f5:cc:31:6a: (0) _9c:01:42:f9:7a:02:61:6d:fe:33:2e:1f:85:9a:d3: (0) _e0:b5:89:ff:0b:38:1d:4f:9f:ee:6e:00:46:37:e1: (0) _bb:91:9d:cf: 76:14:43:c4:e2:33:21:f4:b4:5d:23: (0) _e7:86:d9:73:54:7c:7e:d4:5e:67:63:e1:22:d6:6a: (0) _2f:11:28:e3:0f:68:ef:1f:47:78:e4:98:55:af:af: (0) _54:08:91:ab:be: 24:21:78:59:f0:01:e6:70:b6:da: (0) _18:ae:48:65:e3:e8:2f:d1:bf:66:ca:1c:df:ce:01: (0) _14:51:20:51:5a:62:e4:83:c4:45:67:2a:e2:9d:a2: (0) _d8:1d:89:89:fd: 47:14:db:e6:8d:eb:53:55:89:5e: (0) _c0:70:b8:95:1a:7f:c7:00:b8:7a:3c:a9:be:03:cc: (0) _d8:21:8e:17:16:01:7e:9d:59:20:ef:aa:7d:8e:c4: (0) _3f:18:83:93:4f:ff:68:6e: 57:ae:ec:b7:8e:85:67: (0) _d9:3d (0) _Exponent:_65537_(0x10001) (0)X509v3_EXTENSIONS _ (0)X509v3_Authority_Key_Identifier _keyid:0F:80:61:1C: 82:31:61:D5:2F:28:E7:8D:46:38:B4:2C:E1:C6:D9:E2 (0)X509v3_Subject_Key_Identifier _57:7C:F8:D6:FD:53:52:92:12:99:03:79:B7:5D:F8:9E:18:CB:46:91 (0)X509v3_Subject_Alternative_Name _DNS:archibus.vodacom.co.za,_DNS:archibustest.vodacom.co.za,_DNS:archibusdev.vodacom.co.za (0)X509v3_Key_Usa critical (0) _Digital_Signature,_Key_Encipherment (0)X509v3_Extended_Key_Usage _TLS_Web_Server_Authentication,_TLS_Web_Client_Authentication (0)X509v3_CRL_Distribution_Points (0) _Full_Name: (0) _URI:http://crl3.digicert.com/DigicertSHA2SecureServerCA-1.crl (0) (0) _Full_Name: (0) _URI:http:// crl4.digicert.com/DigicertSHA2SecureServerCA-1.crl (0)X509v3_Certificate_Policies _Policy:_2.23.140.1.2.2 (0) _CPS:_http://www.digicert.com/CPS (0)Authority_Information_Access _OCSP_-_URI:http://ocsp.digicert.com (0) _CA_Issuers_-_URI:http://cacerts.digicert.com/DigiCertSHA2SecureServerCA-2.crt (0)X509v3_Basic_Constraints _CA:FALSE (0)CT_Precertificate_SCTs _Signed_Certificate_Timestamp: (0) _Version_:_v1_(0x0) (0) _Log_ID_:_EE:CD:D0:64:D5: 1A:CE:C5:5C:B7:9D:B4:CD:13:A2: (0) _32:87:46:7C:BC:EC:DE:C3:51:48:59:46:71:1F:B5:9B (0) _Timestamp_:_Aug_11_07:53:07.437_2023_GMT (0) _Extensions:_none (0) _Signature_:_ecdsa-with-SHA256 (0) _30:44:02:20:1C:66:C4:F7:06:8A:11:30:10:90:17:5F: (0) _2E:D9:7B:96:1F:80:16:0A:7E:39:A7:42:61: 24:79: (0) _60:64:13:59:02:20:7F:9C:0B:46:69:F1:D1:52:D5:DB: (0) _C2:90:5E:8D:07:36:59:42:44:A5:10:21:B5:D5:E2:2A: (0) _12:2B:BE:A3:79:F6 (0) _Signed_Certificate_Timestamp: (0) _Version_:_v1_(0x0) (0) _Log_ID_:_48:B0:E3:6B:DA:A6:47:34:0F:E5:6A:02:FA:9D:30:EB: (0) _1C:52:01:CB:56:DD:2C: 81:D9:BB:BF:AB:39:D8:84:73 (0) _Timestamp_:_Aug_11_07:53:07.439_2023_GMT (0) _Extensions:_none (0) _Signature_:_ecdsa-with-SHA256 (0) _30:45:02:20:70:D6:33:72:DD:4A:69:7A:A9:34:BF:72: (0) _71:E0:A8:79:E1:49:E0:B0:2A:45:E7:6F:FB:55:36:CA: (0) _D0:D2:17:8C:02:21:00:AB:FD:F7:70:AC:FF:I 7B:90: (0) _F5:3A:89:BD:F8:C1:4C:D5:1E:AD:03:36:F8:86:4B:26: (0) _15:CF:78:CD:28:BF:FB (0) _Signed_Certificate_Timestamp: (0) _Version_:_v1_(0x0) (0) _Log_ID_:_DA:B6:BF:6B:3F:B5:B6:22:9F:9B:C2:BB:5C:6B:E8:70: (0) _91:71:6C:BB:51:84:85:34:BD:A4:3D:30:48:D7:FB:AB (0) _Timestamp_:_Aug_11_07:53:07.365_2023_GMT (0) _Extensions:_none (0) _Signature_:_ecdsa-with-SHA256 (0) _30:45:02:21:00:82:73:A3:F7:55:A7:B7:B1:D7:19:6F: (0) _1A:B5:29:0A:86:B5:F9:BE:C1:C1:17:27:2C:EB:E0:2B: (0) _DE:71:4D:19:B3:02:20:5D:91:77:0D: 14:C5:43:6F:CB: (0) _FF:D3:70:A7:F6:65:18:08:E8:C6:5F:23:9B:3D:C3:84: (0) _59:64:8E:A0:2B:97:64 (0)Signature (256_octets) (0) ae: 83:b0:2d:c3:df:a7:d2:8a:b0:08:99:9e:28:c8:79 (0) 62:b8:3d:77:de:97:d6:b9:b5:1a:eb:90:a4:64:75:41 (0) 35:95:08:02:61:c7:8c:0c:8a:dd:6b:9b:81:69:9e:f0 (0) b0:df: 03:27:f1:6c:85:c1:04:86:f7:4d:2d:3a:07:f6 (0) 93:5c:f3:aa:66:51:ed:55:48:8e:50:e5:5f:f0:1c:03 (0) c2:83:ff:d2:c5:69:e0:dc:48:28:b3:c8:91:55:4b:a0 (0) 8a:fc:9f:8b: 26:9d:ce:3b:13:c0:d4:9a:a2:bf:a9:6f (0) d2:e7:77:5a:ef:5f:6f:e0:f5:bf:f6:56:58:41:98:ae (0) 0e:39:cf:11:32:16:67:0e:00:b5:ed:9b:54:02:e1:b9 (0) cf:0b: 38:81:13:b4:08:e6:d2:c0:3d:bc:7f:8a:5e:1d (0) f1:55:38:97:04:07:db:62:44:ba:15:df:50:3d:15:06 (0) b7:e5:c4:47:8f:55:a7:98:13:86:08:3c:9d:f9:d9:3a (0) 24:94:0f: 6b:a6:ae:87:3f:1d:71:c3:3f:90:75:c0:96 (0) 2d:dc:90:ee:e6:d3:30:47:68:56:26:2b:d8:18:28:3e (0) c0:11:8c:65:cc:84:dd:b1:f0:24:42:df:eb:d4:7f:b8 (0) 57:a9:21:f1:70:22:f0:7d:c2:25:09:14:04:92:20:40 (1)CERTIFICATE_1 _ (1)Version 3_(0x2) (1)Serial_Number _02:74:2e:aa:17:ca:8e:21:c7:17:bb:1f:fc:fd:0c:a0_ (1)Signature_Algorithm sha256WithRSAEncryption (1)ISSUER_NAME _ countryName US _organizationName DigiCert_Inc _organizationalUnitName www.digicert.com _commonName DigiCert_Global_Root_CA (1)SUBJECT_NAME _ countryName US _organizationName DigiCert_Inc _commonName DigiCert_SHA2_Secure_Server_CA (1)Valid_From Sep_23_00:00:00_2020_GMT (1)Valid_Till Sep_22_23:59:59_2030_GMT (1)Public_Key_Algorithm rsaEncryption (1)RSA_Public_Key (2048_bit) (1) _RSA_Public-Key:_(2048_bit) (1) _Modulus: (1) _00:dc:ae:58:90:4d:c1:c4:30:15:90:35:5b:6e:3c: (1) _82:15:f5:2c 5c:bd:e3:db:ff:71:43:fa:64:25:80: (1) _d4:ee:18:a2:4d:f0:66:d0:0a:73:6e:11:98:36:17: (1) _64:af:37:9d:fd:fa:41:84:af:c7:af:8c:fe:1a:73: (1) _4d:cf: 33:97:90:a2:96:87:53:83:2b:b9:a6:75:48: (1) _2d:1d:56:37:7b:da:31:32:1a:d7:ac:ab:06:f4:aa: (1) _5d:4b:b7:47:46:dd:2a:93:c3:90:2e:79:80:80:ef: (1) _13:04:6a: 14:3b:b5:9b:92:be:c2:07:65:4e:fc:da: (1) _fc:ff:7a:ae:dc:5c:7e:55:31:0c:e8:39:07:a4:d7: (1) _be:2f:d3:0b:6a:d2:b1:df:5f:fe:57:74:53:3b:35: (1) _80:dd:ae:8e: 44:98:b3:9f:0e:d3:da:e0:d7:f4:6b: (1) _29:ab:44:a7:4b:58:84:6d:92:4b:81:c3:da:73:8b: (1) _12:97:48:90:04:45:75:1a:dd:37:31:97:92:e8:cd: (1) _54:0d:3b:e4:c1:3f: 39:5e:2e:b8:f3:5c:7e:10:8e: (1) _86:41:00:8d:45:66:47:b0:a1:65:ce:a0:aa:29:09: (1) _4e:f3:97:eb:e8:2e:ab:0f:72:a7:30:0e:fa:c7:f4: (1) _fd:14:77:c3:a4:5b: 28:57:c2:b3:f9:82:fd:b7:45: (1) _58:9b (1) _Exponent:_65537_(0x10001) (1)X509v3_EXTENSIONS _ (1)X509v3_Subject_Key_Identifier _0F:80:61:1C: 82:31:61:D5:2F:28:E7:8D:46:38:B4:2C:E1:C6:D9:E2 (1)X509v3_Authority_Key_Identifier _keyid:03:DE:50:35:56:D1:4C:BB:66:F0:A3:E2:1B:1B:C3:97:B2:3D:D1:5 (1)X509v3_Key_Usage critical (1) _Digital_Signature,_Certificate_Sign,_CRL_Sign (1)X509v3_Extended_Key_Usage _TLS_Web_Server_Authentication,_TLS_Web_Client_Authentication (1)X509v3_Basic_Constraints critical (1) _CA:TRUE,_pathlen:0 (1)Authority_Information_Access _OCSP_-_URI:http://ocsp.digicert.com (1) _CA_Issuers_-_URI:http://cacerts.digicert.com/DigiCertGlobalRootCA.crt (1)X509v3_CRL_Distribution_Points (1) _Full_Name: (1) _URI:http://crl3.digicert.com/DigiCertGlobalRootCA.crl (1) (1) _Full_Name: (1) _URI:http://crl4.digicert.cor DigiCertGlobalRootCA.crl (1)X509v3_Certificate_Policies _Policy:_2.23.140.1.1 (1) _Policy:_2.23.140.1.2.1 (1) _Policy:_2.23.140.1.2.2 (1) _Policy:_2.23.140.1.2.3 (1)Signature (256_octets) (1) 77:31:1f:08:97:d7:12:9b:63:d2:11:65:08:a6:f6:65 (1) b9:b8:fa:92:03:cb:a1:7e:e1:c8:0d:8c:3e:b4:1b:91 (1) be:02:08:5e:9f:59:71:7b: 11:fd:e0:c0:e3:8f:59:d7 (1) a0:52:a1:d0:4b:54:d2:48:96:48:ef:77:e9:29:06:cb (1) 43:10:a0:2f:3c:16:8e:2d:fe:1e:55:3c:ec:c3:98:ee (1) 18:0d:23:e8:07:f5:b3:2d:c4:ab 57:73:5a:f6:1b:53 (1) ba:fb:1f:fa:bd:8c:d3:51:51:20:47:5e:ef:7f:98:ab (1) 17:42:ca:85:5c:9f:22:37:34:45:76:f2:43:5e:00:9e (1) 22:83:ac:df:af:d1:e6:c7:13:17:e9:a4:69:64:4c:80 (1) 67:ea:b6:a4:7f:8f:7d:e1:51:fa:9e:97:67:ea:69:2e (1) b3:90:a4:1c:15:c8:ac:cb:4f:29:ec:7a:5c:5d:9f:8a (1) b8:d4:0c:bb:94:ee:d0:bc:cb:b5:a5:1e:08:cf:c4:41 (1) 03:0d:bd:06:c3:a0:f4:c8:37:55:4a:f1:bf:e5:79:42 (1) 35:ab:41:98:ef:fc:13:39:c3:bb:5b:eb:ef:63:7c:80 (1) 9c:c8:49:46:70:6b:a0:82:50:3e:d0:04:b6:ca:25:c5 (1) c1:05:55:5f:f2:7c:2f:57:d1:af:95:6f:ac:6d:79:6b (2)CERTIFICATE_2 _ (2)Version 3_(0x2) (2)Serial_Number _08:3b:e0:56:90:42:46:b1:a1:75:6a:c9:59:91:c7:4a_ (2)Signature_Algorithm sha1WithRSAEncryption (2)ISSUER_NAME _ countryName US _organizationName DigiCert_Inc _organizationalUnitName www.digicert.com _commonName DigiCert_Global_Root_CA (2)SUBJECT_NAME _ countryName US _organizationName DigiCert_Inc _organizationalUnitName www.digicert.com _commonName DigiCert_Global_Root_CA (2)Valid_From Nov_10_00:00:00_2006_GMT (2)Valid_Till Nov_10_00:00:00_2031_GMT (2)Public_Key_Algorithm rsaEncryption (2)RSA_Public_Key (2048_bit) (2) _RSA_Public-Key:_(2048_bit) (2) _Modulus: (2) _00:e2:3b:e1:11:72:de:a8:a4:d3:a3:57:aa:50:a2: (2) _8f:0b:77:90:c9:a2:a5:ee:12:ce:96:5b:01:09:20: (2) _cc:01:93:a7:4e:30:b7:53:f7:43:c4:69:00:57:9d: (2) _e2:8d 22:dd:87:06:40:00:81:09:ce:ce:1b:83:bf: (2) _df:cd:3b:71:46:e2:d6:66:c7:05:b3:76:27:16:8f: (2) _7b:9e:1e:95:7d:ee:b7:48:a3:08:da:d6:af:7a:0c: (2) _39:06:65:7f:4a 5d:1f:bc:17:f8:ab:be:ee:28:d7: (2) _74:7f:7a:78:99:59:85:68:6e:5c:23:32:4b:bf:4e: (2) _c0:e8:5a:6d:e3:70:bf:77:10:bf:fc:01:f6:85:d9: (2) _a8:44:10:58:32:a9:75:18:d5:d1:a2:be:47:e2:27: (2) _6a:f4:9a:33:f8:49:08:60:8b:d4:5f:b4:3a:84:bf: (2) _a1:aa:4a:4c:7d:3e:cf:4f:5f:6c:76:5e:a0:4b:37: (2) _91:9e:dc 22:e6:6d:ce:14:1a:8e:6a:cb:fe:cd:b3: (2) _14:64:17:c7:5b:29:9e:32:bf:f2:ee:fa:d3:0b:42: (2) _d4:ab:b7:41:32:da:0c:d4:ef:f8:81:d5:bb:8d:58: (2) _3f:b5:1b:e8:49:28:a2:70:da:31:04:dd:f7:b2:16: (2) _f2:4c:0a:4e:07:a8:ed:4a:3d:5e:b5:7f:a3:90:c3: (2) _af:27 (2) _Exponent:_65537_(0x10001) (2)X509v3_EXTENSIONS _ (2)X509v3_Key_Usage critical (2) _Digital_Signature,_Certificate_Sign,_CRL_Sign (2)X509v3_Basic_Constraints critical (2) _CA:TRU (2)X509v3_Subject_Key_Identifier _03:DE:50:35:56:D1:4C:BB:66:F0:A3:E2:1B:1B:C3:97:B2:3D:D1:55 (2)X509v3_Authority_Key_Identifier _keyid:03:DE: 50:35:56:D1:4C:BB:66:F0:A3:E2:1B:1B:C3:97:B2:3D:D1:55 (2)Signature (256_octets) (2) cb:9c:37:aa:48:13:12:0a:fa:dd:44:9c:4f:52:b0:f4 (2) df:ae: 04:f5:79:79:08:a3:24:18:fc:4b:2b:84:c0:2d (2) b9:d5:c7:fe:f4:c1:1f:58:cb:b8:6d:9c:7a:74:e7:98 (2) 29:ab:11:b5:e3:70:a0:a1:cd:4c:88:99:93:8c:91:70 (2) e2:ab:0f:1c: 93:a9:ff:63:d5:e4:07:60:d3:a3:bf (2) 9d:5b:09:f1:d5:8e:e3:53:f4:8e:63:fa:3f:a7:db:b4 (2) 66:df:62:66:d6:d1:6e:41:8d:f2:2d:b5:ea:77:4a:9f (2) 9d:58:e2:2b: 59:c0:40:23:ed:2d:28:82:45:3e:79:54 (2) 92:26:98:e0:80:48:a8:37:ef:f0:d6:79:60:16:de:ac (2) e8:0e:cd:6e:ac:44:17:38:2f:49:da:e1:45:3e:2a:b9 (2) 36:53:cf:3a: 50:06:f7:2e:e8:c4:57:49:6c:61:21:18 (2) d5:04:ad:78:3c:2c:3a:80:6b:a7:eb:af:15:14:e9:d8 (2) 89:c1:b9:38:6c:e2:91:6c:8a:ff:64:b9:77:25:57:30 (2) c0:1b:

24:a3:e1:dc:e9:df:47:7c:b5:b4:24:08:05:30 (2) ec:2d:bd:0b:bf:45:bf:50:b9:a9:f3:eb:98:01:12:ad (2) c8:88:c6:98:34:5f:8d:0a:3c:c6:e9:d5:95:95:6d:de #table cols="2
NAME VALUE (0)CERTIFICATE_0 _ (0)Version 3_(0x2) (0)Serial_Number _01:8c:fc:40:a6:82:cc:44:37:35:84:76:9e:2f:e7:2a_ (0)Signature_Algorithm
sha256WithRSAEncryption (0)ISSUER_NAME _ countryName BE _organizationName GlobalSign_nv-sa _commonName
GlobalSign_Atlas_R3_DV_TLS_CA_2024_Q1 (0)SUBJECT_NAME _ commonName imperva.com (0)Valid_From Jan_18_13:49:41_2024_GMT (0)Valid_Till
Jul_16_13:49:41_2024_GMT (0)Public_Key_Algorithm rsaEncryption (0)RSA_Public_Key (2048_bit) (0) _RSA_Public-Key:_(2048_bit) (0) _Modulus: (0)
_00:b4:45:53:af:8c:d2:ca:21:2c:0c:a2:ea:0d:53: (0) _f4:17:ae:ad:ab:28:95:7d:5f:31:74:3d:7d:1a:3f: (0) _d6:c8:3c:cc:bc:b0:bb:ce:42:2f:cb:76:73:fb:3b: (0) _ef:44:8
4a:30:61:c0:c1:7f:6e:f9:03:e2:c8: (0) _0c:98:5a:b0:c4:00:47:93:dc:84:89:e4:50:91:09: (0) _39:a8:45:f1:97:61:4d:82:a4:4c:ce:d9:71:fd:01: (0) _e0:9f:
57:fa:c1:5a:da:ee:a1:6a:94:86:bd:20:93: (0) _e5:14:ed:60:6d:3e:db:a5:c2:cc:85:24:64:16:62: (0) _88:34:c1:12:7f:bc:f7:8c:8e:76:32:30:9d:dd:79: (0)
_7b:b0:4a:f6:38:f5:bc:ef:a8:99:cc:c3:15:ca:a9: (0) _0a:db:e1:64:71:fc:13:0b:6c:e8:4a:63:8e:f9:a8: (0) _3c:bb:ed:78:70:ab:3c:bd:27:e7:38:61:8a:2a:3b: (0)
_51:67:00:70:99:88:af:4b:ae:35:17:e0:83:02:34: (0) _f5:13:b1:96:16:41:50:60:99:41:39:fb:01:b0:4f: (0) _71:ad:20:53:dd:ad:8b:1d:aa:eb:06:40:bc:9c:08: (0) _9d:8
0d:bb:33:6d:f4:91:a7:80:0f:4e:c9:29:6b: (0) _0d:34:6a:14:a8:62:72:bd:a9:92:29:c5:29:ec:d8: (0) _1b:47 (0) _Exponent:_65537_(0x10001) (0)X509v3_EXTENSIO
_ (0)X509v3_Subject_Alternative_Name
_DNS:lending.vodacom.co.za,_DNS:hyperbook.vodacom.co.za,_DNS:journalist.vodacom.co.za,_DNS:de.c3dcrm.ppiam.vodacom.co.za,_DNS:nc.m2.ppret.voda
pwmicros.vodacom.co.za,_DNS:m2d.ret.vodacom.co.za,_DNS:kw3118.vod (0)
acom.co.za,_DNS:ciims.vodacom.co.za,_DNS:ifsfsmqa.vodacom.co.za,_DNS:cdn.mobucks.vodacom.co.za,_DNS:apix.vodacom.co.za,_DNS:nc.m2d.iam.vodac
ubuntu.vodacom.co.ls,_DNS:business.vodacom.co.za,_DNS:cc.m2d.ret.vodacom.co.za,_DNS:cc.m2.ppret.vodacom.co.za,_DNS:mobucks.sso. (0)
vodacom.co.za,_DNS:next.vodacom.co.za,_DNS:ifsfsm.vodacom.co.za,_DNS:cognosqa.sso.vodacom.co.za,_DNS:fr.m2.iam.vodacom.co.za,_DNS:nc.m2.iam.v
crm1.vodacom.co.za,_DNS:aplus-
dev.vodacom.co.za,_DNS:sorteos.mivodafoneapp.es,_DNS:login.ret.vodacom.co.za,_DNS:fr.m2d.ppret.vodacom.co.za,_DNS:etomrsso.vodacom.co.za,_DNS:fr
(0) nts.vodacom.co.za,_DNS:de.m2d.ppret.vodacom.co.za,_DNS:lendingdev.vodacom.co.za,_DNS:c3d-
crm.vodacom.co.za,_DNS:engageplatform.vodacom.co.za,_DNS:archibus.vodacom.co.za,_DNS:dwp.vodacom.co.za,_DNS:mobucks.ppent.vodacom.co.za,_DN
(0) _DNS:hcsadminapi.voicespend.vodacom.co.za,_DNS:m2.ppret.vodacom.co.za,_DNS:aplus-
qa.vodacom.co.za,_DNS:login.ent.vodacom.co.za,_DNS:de.c3dcrm.iam.vodacom.co.za,_DNS:public.tobicloud-
dev.vodafone.it,_DNS:consent.ppsso.vodacom.co.za,_DNS:*.to-
zi.com,_DNS:cc.m2d.iam.vodacom.co.za,_DNS:cc.m2.ppiam.vodacom.co.za,_DNS:login.thanos.co.za,_DNS:bcmapp.vodacom.co.za,_DNS:irsp.iam.vodacom.c
zi.com,_DNS:lendingqa.vodacom.co.za (0)X509v3_Key_Usage critical (0) _Digital_Signature,_Key_Encipherment (0)X509v3_Extended_Key_Usage
_TLS_Web_Server_Authentication,_TLS_Web_Client_Authentication (0)X509v3_Subject_Key_Identifier _2D:75:CE:D0:C6:36:E7:0A:AA:
02:47:60:D3:D3:07:25:22:48:58:17 (0)X509v3_Certificate_Policies _Policy:_2.23.140.1.2.1 (0) _Policy:_1.3.6.1.4.1.4146.10.1.3 (0) _CPS:_https://
www.globalsign.com/repository/ (0)X509v3_Basic_Constraints critical (0) _CA:FALSE (0)Authority_Information_Access _OCSP_-_URI:http://ocsp.globalsign.com
gsatlasr3dvtlsca2024q1 (0) _CA_Issuers_-_URI:http://secure.globalsign.com/cacert/gsatlasr3dvtlsca2024q1.crt (0)X509v3_Authority_Key_Identifier _keyid:
66:C0:C7:A3:9A:CD:FE:F3:EA:CE:4B:53:0B:61:5E:AF:33:05:B3:E1 (0)X509v3_CRL_Distribution_Points (0) _Full_Name: (0) _URI:http://crl.globalsign.com/ca/
gsatlasr3dvtlsca2024q1.crl (0)CT_Precertificate_SCTs _Signed_Certificate_Timestamp: (0) _Version_:_v1_(0x0) (0) _Log_ID_:_76:FF:88:3F:0A:B6:FB:
95:51:C2:61:CC:F5:87:BA:34: (0) _B4:A4:CD:BB:29:DC:68:42:0A:9F:E6:67:4C:5A:3A:74 (0) _Timestamp_:_Jan_18_13:50:14.915_2024_GMT (0)
_Extensions:_none (0) _Signature_:_ecdsa-with-SHA256 (0) _30:45:02:20:2A:87:69:07:90:39:65:94:75:77:FF:D0: (0) _36:EF:3A:28:9F:5B:44:AD:9D:34:CC:7F:
70:D1:22:2D: (0) _1D:BB:0B:09:02:21:00:A1:47:3B:73:1C:9B:16:4F:E7: (0) _21:3D:DA:DE:02:27:B5:7E:5D:D8:76:30:7E:97:0B:76: (0) _1A:51:40:FC:60:E3:B5 (0
_Signed_Certificate_Timestamp: (0) _Version_:_v1_(0x0) (0) _Log_ID_:_3B:53:77:75:3E:2D:B9:80:4E:8B:30:5B:06:FE:40:3B: (0) _67:D8:4F:C3:F4:C7:BD:00:0
72:6F:E1:FA:D4:17 (0) _Timestamp_:_Jan_18_13:50:15.031_2024_GMT (0) _Extensions:_none (0) _Signature_:_ecdsa-with-SHA256 (0)
_30:45:02:20:08:14:0B:B5:56:12:65:11:C8:E1:F3:AC: (0) _E8:FF:94:C8:5E:A0:2D:F7:7E:7B:13:6F:CA:64:CE:0E: (0) _18:F2:49:2C:02:21:00:E6:E6:BB:AF:89:7E
02:33:44: (0) _19:4C:6A:22:98:CD:E1:61:36:C0:FA:58:92:BB:E8:32: (0) _1C:E2:2F:11:B1:D3:D4 (0) _Signed_Certificate_Timestamp: (0) _Version_:_v1_(0x0) (0
_Log_ID_:_48:B0:E3:6B:DA:A6:47:34:0F:E5:6A:02:FA:9D:30:EB: (0) _1C:52:01:CB:56:DD:2C:81:D9:BB:BF:AB:39:D8:84:73 (0)
Timestamp:_Jan_18_13:50:15.338_2024_GMT (0) _Extensions:_none (0) _Signature_:_ecdsa-with-SHA256 (0) _30:45:02:21:00:83:84:EC:EF:2B:
59:53:02:10:C9:3C: (0) _0E:99:97:D8:50:35:1C:E5:9B:7F:46:01:8C:44:B2:F9: (0) _23:3E:9D:DB:CB:02:20:47:02:FE:EC:BD:B4:D5:1D:49: (0) _FF:17:9F:
01:12:47:EA:AA:E0:A8:72:E8:21:49:43:6D: (0) _CC:9F:4C:C2:42:16:73 (0)Signature (256_octets) (0) 7a:c3:19:8f:f8:f8:52:33:00:a5:aa:ef:21:09:db:48 (0)
a0:d3:62:75:cc:48:c4:2d:ed:84:27:95:28:cd:30:d4 (0) 11:2a:65:8b:83:ea:21:d8:1b:d2:4f:01:10:35:01:dd (0) e8:65:c1:a4:4a:64:06:46:24:a6:65:45:38:f9:6c:3b (0)
85:11:80:65:84:40:97:16:25:bf:c0:26:75:6d:6c:4c (0) a2:0d:ea:d4:16:f1:be:72:3b:da:a7:50:43:7d:22:18 (0) 3f:43:88:2e:9b:dd:53:9e:8f:28:88:84:d6:d9:be:77 (0) 2d
66:d1:f1:25:7a:ba:00:40:2f:11:67:98:81:ab (0) 04:21:79:dd:b0:6b:c1:f1:b5:f1:7e:89:72:fc:55:39 (0) 7c:3e:53:2d:c5:d3:fb:e3:43:b7:ae:06:f3:98:1a:41 (0) 8d:
5d:e2:80:84:dc:a5:7d:92:5f:d1:e5:1a:d2:c8:50 (0) 32:18:97:54:31:1b:70:1f:7d:5c:08:23:6f:e3:c9:9f (0) b8:81:c0:36:af:60:19:7a:8b:94:15:2b:9f:82:b4:81 (0)
43:2b:b0:c5:93:08:e5:23:41:d9:c4:60:0e:9c:00:d3 (0) 23:e3:ff:70:29:cb:3a:c7:16:dc:0a:e8:a3:f8:1c:8c (0) b1:f0:0d:cb:46:4d:96:41:d7:b2:44:c3:81:be:99:b9
(1)CERTIFICATE_1 _ (1)Version 3_(0x2) (1)Serial_Number _7f:b6:a0:ea:55:e2:8c:04:4c:95:2e:95:d6:34:9f:5c_ (1)Signature_Algorithm sha256WithRSAEncryptio
(1)ISSUER_NAME _ organizationalUnitName GlobalSign_Root_CA_-_R3 _organizationName GlobalSign _commonName GlobalSign (1)SUBJECT_NAME _
countryName BE _organizationName GlobalSign_nv-sa _commonName GlobalSign_Atlas_R3_DV_TLS_CA_2024_Q1 (1)Valid_From Oct_18_04:09:32_2023_G
(1)Valid_Till Oct_18_00:00:00_2025_GMT (1)Public_Key_Algorithm rsaEncryption (1)RSA_Public_Key (2048_bit) (1) _RSA_Public-Key:_(2048_bit) (1) _Modulu
(1) _00:94:46:a2:54:17:05:2e:68:70:09:bf:bd:79:95: (1) _0d:cb:1b:a8:dd:d7:5f:d6:a0:2a:a1:2f:47:45:4a: (1) _7a:6c:7b:f9:d0:3a:cf:3c:43:68:9e:2f:48:c7:82: (1) _55:
43:94:25:1b:f4:f0:f3:94:ab:01:86:f9:42: (1) _6b:b7:45:7d:fd:43:31:6f:dd:28:d8:84:48:0c:af: (1) _d0:b8:db:ab:af:7e:86:39:b3:18:5b:e2:bc:6c:d3: (1) _06:d1:12:86:22
8a:56:a6:4c:a8:56:81:3e:38: (1) _c6:99:66:44:3e:c9:70:58:38:fc:a9:bb:72:c2:83: (1) _b6:4c:c9:cc:a6:9c:4d:3b:29:a6:b3:a3:34:96:29: (1) _50:9c:12:b5:c9:a6:22:5d
18:d0:8c:ef:04:c2:43: (1) _8c:f7:98:8a:95:7c:74:6b:12:47:51:94:b9:9c:f9: (1) _04:be:ba:a9:ca:38:22:b2:40:ca:d8:44:db:e3:1a: (1)
_66:13:64:40:41:70:17:c4:cd:c5:a6:79:fd:93:13: (1) _22:d5:ab:7c:02:1b:16:c4:23:3f:a4:db:9c:53:aa: (1) _db:e2:ea:a2:6e:9f:4a:6d:b0:1d:84:3c:9d:fa:c2: (1)
_3a:bc:f6:43:4b:e4:6d:3a:6b:fe:6d:37:5a:00:f5: (1) _03:78:37:38:01:5e:ff:37:47:4e:54:c8:20:0a:9e: (1) _20:0f (1) _Exponent:_65537_(0x10001)
(1)X509v3_EXTENSIONS _ (1)X509v3_Key_Usage critical (1) _Digital_Signature,_Certificate_Sign,_CRL_Sign (1)X509v3_Extended_Key_Usage
_TLS_Web_Server_Authentication,_TLS_Web_Client_Authentication (1)X509v3_Basic_Constraints critical (1) _CA:TRUE,_pathlen:0
(1)X509v3_Subject_Key_Identifier _66:C0:C7:A3:9A:CD:FE:F3:EA:CE:4B:53:0B:61:5E:AF:33:05:B3:E1 (1)X509v3_Authority_Key_Identifier _keyid:8F:F0:4B:
7F:A8:2E:45:24:AE:4D:50:FA:63:9A:8B:DE:E2:DD:1B:BC (1)Authority_Information_Access _OCSP_-_URI:http://ocsp2.globalsign.com/rootr3 (1) _CA_Issuers_-
_URI:http://secure.globalsign.com/cacert/root-r3.crt (1)X509v3_CRL_Distribution_Points (1) _Full_Name: (1) _URI:http://crl.globalsign.com/root-r3.crl
(1)X509v3_Certificate_Policies _Policy:_2.23.140.1.2.1 (1) _Policy:_1.3.6.1.4.1.4146.10.1.3 (1)Signature (256_octets) (1) 1d:5a:11:af:98:37:f5:8f:fd:1c:c5:7c:
07:c5:69:fe (1) 00:b8:b2:af:a3:4c:86:88:27:0a:48:3d:17:34:0e:77 (1) 2f:8f:12:70:0d:47:2b:84:a4:8c:0b:e2:f1:64:fd:07 (1) c4:27:1e:7f:ee:e2:5d:0c:
33:33:f4:56:e0:33:f4:02 (1) 8e:be:be:19:75:88:b7:c5:c5:d0:7b:6a:da:a6:de:93 (1) c0:c6:c8:8c:be:f3:e4:96:ac:e5:9b:0d:9e:9c:27:e3 (1) b5:ae:63:03:97:ea:
89:28:a2:f1:35:c9:f1:67:86:d5 (1) 0c:44:8b:3a:8d:b2:ae:c2:fb:bc:bd:39:89:72:19:77 (1) 40:60:00:38:bb:c1:db:e2:0b:b9:e7:dc:da:3b:05:fc (1) bd:94:c2:9a:31:b7:bb:
2b:a7:6f:f5:41:33:38:aa (1) bc:d6:4f:d7:24:46:da:04:07:31:88:9a:1f:aa:e4:9d (1) c2:9e:30:4f:5f:dd:2a:d9:7d:8a:a9:13:fe:c6:23:ec (1) 17:5b:42:1a:6a:dc:ec:
09:d8:a6:2f:aa:cb:ae:4f:1a (1) 15:68:20:ee:c4:bf:dc:c8:ed:47:25:eb:c2:3f:de:b9 (1) aa:05:a8:4b:47:f2:81:d6:2b:18:0a:cd:1c:e7:b5:c6 (1) fa:93:26:67:5e:0a:af:
85:82:2e:e1:1f:5c:43:3c:b1

Info List

Info #1

Certificate Fingerprint:0152F86354FCA9525B280C233F7DA6CF8B5F2373C42644723226AE67238DB190

WAS Web Application Report

Security Weaknesses (15)

150210 Information Disclosure via Response Header (1)

150210 Information Disclosure via Response Header

archibus.vodacom.co.za/archibus

Finding #	14172489	**Severity**	Information Gathered - Level 3
Unique #	944eefc4-3d52-485b-b5fa-8ffb2fad58e0		
Group	Security Weaknesses		
CWE	CWE-16, CWE-201	**Detection Date**	11 Feb 2024 21:02 GMT+0200
OWASP	A5 Security Misconfiguration		
WASC	WASC-15 APPLICATION MISCONFIGURATION		

Details

Threat

HTTP response headers like 'Server', 'X-Powered-By', 'X-AspNetVersion', 'X-AspNetMvcVersion' could disclose information about the platform and technologies used by the website. The HTTP response include one or more such headers.

Impact

The headers can potentially be used by attackers for fingerprinting and launching attacks specific to the technologies and versions used by the web application. These response headers are not necessary for production sites and should be disabled.

Solution

Disable such response headers, remove them from the response, or make sure that the header value does not contain information which could be used to fingerprint the server-side components of the web application.

Results

One or more response headers disclosing information about the application platform were present on the following pages:
(Only first 50 such pages are reported)

GET https://archibus.vodacom.co.za/FPRWin/index.aspx response code: 401
Server: Microsoft-IIS/10.0
X-Powered-By: ASP.NET

GET https://archibus.vodacom.co.za/FPRWin/ response code: 401
Server: Microsoft-IIS/10.0
X-Powered-By: ASP.NET

150261 Subresource Integrity (SRI) Not Implemented (1)

150261 Subresource Integrity (SRI) Not Implemented

archibus.vodacom.co.za/archibus

Finding #	10510597	**Severity**	Information Gathered - Level 3
Unique #	0466d4c0-4cb9-4c81-8095-f7dc1a65697e		
Group	Security Weaknesses		
CWE	CWE-693	**Detection Date**	11 Feb 2024 21:02 GMT+0200
OWASP	-		
WASC	-		

Details

Threat

The integrity attribute is missing in script and/or link elements. Subresource Integrity (SRI) is a standard browser security feature that verifies the value of the integrity attribute in

Impact

Absence of SRI checks means it is impossible to verify that the third-party resources are delivered without any unexpected manipulation.

Solution

All script and link elements that load external content should include the integrity attribute to ensure that the content is trustworthy.

More information:
Subresource Integrity article by Mozilla
OWASP Third-Party JavaScript Management Cheat Sheet

Results

Externally loaded Javascript and CSS resources without integrity checks:

Parent link : https://archibus.vodacom.co.za/_Incapsula_Resource?CWUDNSAI=23&xinfo=13-50005422-0%200NNN%20RT%281684091004823%2015780%29%20q%280%20-1%20-1%201%29%20r%280%20-1%29%20B15%284%2C200%2C0%29%20U18&incident_id=768000330126840138-244105402621364301&edet=15&cinfo=04000000&rpinfo=0&mth=GET
Found following resource links without integrity checks (only first 10 links are reported)
https://fonts.googleapis.com/css2?family=Inter:wght@300;400;500;700&display=swap

Parent link : https://archibus.vodacom.co.za/_Incapsula_Resource?CWUDNSAI=23&xinfo=13-51475396-0%200NNN%20RT%281696791744809%202625%29%20q%280%20-1%20-1%202%29%20r%280%20-1%29%20B15%284%2C200%2C0%29%20U18&incident_id=764000460129603047-261986575540030349&edet=15&cinfo=04000000&rpinfo=0&mth=GET
Found following resource links without integrity checks (only first 10 links are reported)
https://fonts.googleapis.com/css2?family=Inter:wght@300;400;500;700&display=swap

Parent link : https://archibus.vodacom.co.za/_Incapsula_Resource?CWUDNSAI=23&xinfo=14-178098704-0%200NNN%20RT%281681066855737%202281%29%20q%280%20-1%20-1%208%29%20r%280%20-1%29%20B15%284%2C200%2C0%29%20U18&incident_id=766000980317811993-862742334339422350&edet=15&cinfo=04000000&rpinfo=0&mth=GET
Found following resource links without integrity checks (only first 10 links are reported)
https://fonts.googleapis.com/css2?family=Inter:wght@300;400;500;700&display=swap

Parent link : https://archibus.vodacom.co.za/_Incapsula_Resource?CWUDNSAI=23&xinfo=13-51475397-0%200NNN%20RT%281696791744809%2015891%29%20q%280%20-1%20-1%200%29%20r%280%20-1%29%20B15%284%2C200%2C0%29%20U18&incident_id=764000460129603047-262001204198640525&edet=15&cinfo=04000000&rpinfo=0&mth=GET
Found following resource links without integrity checks (only first 10 links are reported)
https://fonts.googleapis.com/css2?family=Inter:wght@300;400;500;700&display=swap

Parent link : https://archibus.vodacom.co.za/_Incapsula_Resource?CWUDNSAI=23&xinfo=14-178098704-0%200NNN%20RT%281681066855737%202281%29%20q%280%20-1%20-1%208%29%20r%280%20-1%29%20B15%284%2c200%2c0%29%20U18&incident_id=766000980317811993-862742334339422350&edet=15&cinfo=04000000&rpinfo=0&mth=GET
Found following resource links without integrity checks (only first 10 links are reported)
https://fonts.googleapis.com/css2?family=Inter:wght@300;400;500;700&display=swap

Parent link : https://archibus.vodacom.co.za/_Incapsula_Resource?CWUDNSAI=23&xinfo=14-178100241-0%200NNN%20RT%281681066864525%202%29%20q%280%20-1%20-1%200%29%20r%280%20-1%29%20B15%284%2c200%2c0%29%20U18&incident_id=766000980317811993-862747269256845454&edet=15&cinfo=04000000&rpinfo=0&mth=GET
Found following resource links without integrity checks (only first 10 links are reported)
https://fonts.googleapis.com/css2?family=Inter:wght@300;400;500;700&display=swap

Parent link : https://archibus.vodacom.co.za/_Incapsula_Resource?CWUDNSAI=23&xinfo=14-56552041-0%200NNN%20RT%281684091004822%202271%29%20q%280%20-1%20-1%200%29%20r%280%20-1%29%20B15%284%2C200%2C0%29%20U18&incident_id=768000330126840138-290605261188499534&edet=15&cinfo=04000000&rpinfo=0&mth=GET
Found following resource links without integrity checks (only first 10 links are reported)
https://fonts.googleapis.com/css2?family=Inter:wght@300;400;500;700&display=swap

Parent link : https://archibus.vodacom.co.za/_Incapsula_Resource?CWUDNSAI=23&xinfo=14-99580654-0%200NNN%20RT%281694372525149%204%29%20q%280%20-1%20-1%200%29%20r%280%20-1%29%20B15%284%2c200%2c0%29%20U18&incident_id=764000410179907764-464701605912775246&edet=15&cinfo=04000000&rpinfo=0&mth=GET
Found following resource links without integrity checks (only first 10 links are reported)
https://fonts.googleapis.com/css2?family=Inter:wght@300;400;500;700&display=swap

Parent link : https://archibus.vodacom.co.za/_Incapsula_Resource?CWUDNSAI=23&xinfo=14-99576411-0%200NNN%20RT%281694372512606%209%29%20q%280%20-1%20-1%20-1%29%20r%280%20-1%29%20B15%284%2c200%2c0%29%20U18&incident_id=764000410179907764-464681797523606094&edet=15&cinfo=04000000&rpinfo=0&mth=GET
Found following resource links without integrity checks (only first 10 links are reported)
https://fonts.googleapis.com/css2?family=Inter:wght@300;400;500;700&display=swap

Parent link : https://archibus.vodacom.co.za/_Incapsula_Resource?CWUDNSAI=23&xinfo=4-185001335-0%200NNN%20RT%281688929350663%207%29%20q%280%20-1%20-1%20-1%29%20r%280%20-1%29%20B15%284%2c200%2c0%29%20U18&incident_id=449001580571594800-9499091938071776048&edet=15&cinfo=04000000&rpinfo=0&mth=GET
Found following resource links without integrity checks (only first 10 links are reported)
https://fonts.googleapis.com/css2?family=Inter:wght@300;400;500;700&display=swap

Parent link : https://archibus.vodacom.co.za/_Incapsula_Resource?CWUDNSAI=23&xinfo=4-6583483-0%200NNN%20RT%2816967916769 41%203%29%20q%280%20-1%20-1%20-1%29%20r%280%20-1%29%20B15%284%2c200%2c0%29%20U18&incident_id=764000460129603047-340597864920544 04&edet=15&cinfo=04000000&rpinfo=0&mth=GET
Found following resource links without integrity checks (only first 10 links are reported)
https://fonts.googleapis.com/css2?family=Inter:wght@300;400;500;700&display=swap

Parent link : https://archibus.vodacom.co.za/_Incapsula_Resource?CWUDNSAI=23&xinfo=4-9346511-0%200NNN%20RT%281694372516064%2015875%29%20q%280%20-1%20-1%200%29%20r%280%20-1%29%20B15%284%2C200%2C0%29%20U18&incident_id=764000410179907764-456022061573760 68&edet=15&cinfo=04000000&rpinfo=0&mth=GET
Found following resource links without integrity checks (only first 10 links are reported)
https://fonts.googleapis.com/css2?family=Inter:wght@300;400;500;700&display=swap

Parent link : https://archibus.vodacom.co.za/_Incapsula_Resource?CWUDNSAI=23&xinfo=4-77155952-0%200NNN%20RT%281699815748753%203%29%20q%280%20-1%20-1%200%29%20r%280%20-1%29%20B15%284%2c200%2c0%29%20U18&incident_id=766001190516980779-434236724277550532&edet=15&cinfo=04000000&rpinfo=0&mth=GET
Found following resource links without integrity checks (only first 10 links are reported)
https://fonts.googleapis.com/css2?family=Inter:wght@300;400;500;700&display=swap

Parent link : https://archibus.vodacom.co.za/_Incapsula_Resource?CWUDNSAI=23&xinfo=5-218372829-0%200NNN%20RT%281688929454117%202786%29%20q%280%20-1%20-1%201%29%20r%280%20-1%29%20B15%284%2C200%2C0%29%20U18&incident_id=449001580571594800-1118955442970634117&edet=15&cinfo=04000000&rpinfo=0&mth=GET
Found following resource links without integrity checks (only first 10 links are reported)
https://fonts.googleapis.com/css2?family=Inter:wght@300;400;500;700&display=swap

Parent link : https://archibus.vodacom.co.za/_Incapsula_Resource?CWUDNSAI=23&xinfo=5-102401836-0%200NNN%20RT%281686510484694%203%29%20q%280%20-1%20-1%20-1%29%20r%280%20-1%29%20B15%284%2c200%2c0%29%20U18&incident_id=769009803598071 66-486662297683564677&edet=15&cinfo=04000000&rpinfo=0&mth=GET
Found following resource links without integrity checks (only first 10 links are reported)
https://fonts.googleapis.com/css2?family=Inter:wght@300;400;500;700&display=swap

Parent link : https://archibus.vodacom.co.za/_Incapsula_Resource?CWUDNSAI=23&xinfo=5-218374445-0%200NNN%20RT%281688929463409%203%29%20q%280%20-1%20-1%200%29%20r%280%20-1%29%20B15%284%2c200%2c0%29%20U18&incident_id=449001580571594800-1118961528939292549&edet=15&cinfo=04000000&rpinfo=0&mth=GET
Found following resource links without integrity checks (only first 10 links are reported)
https://fonts.googleapis.com/css2?family=Inter:wght@300;400;500;700&display=swap

Parent link : https://archibus.vodacom.co.za/_Incapsula_Resource?CWUDNSAI=23&xinfo=6-59075188-0%200NNN%20RT%281699815693202%203%29%20q%280%20-1%20-1%20-1%29%20r%280%20-1%29%20B15%284%2c200%2c0%29%20U18&incident_id=766001190516980779-333163456469278150&edet=15&cinfo=04000000&rpinfo=0&mth=GET
Found following resource links without integrity checks (only first 10 links are reported)
https://fonts.googleapis.com/css2?family=Inter:wght@300;400;500;700&display=swap

Parent link : https://archibus.vodacom.co.za/_Incapsula_Resource?CWUDNSAI=23&xinfo=7-120841300-0%200NNN%20RT%281688929454097%2014%29%20q%280%20-1%20-1%20-1%29%20r%280%20-1%29%20B15%284%2C200%2C0%29%20U18&incident_id=449001580571594800-6317292161315081 03&edet=15&cinfo=04000000&rpinfo=0&mth=GET
Found following resource links without integrity checks (only first 10 links are reported)
https://fonts.googleapis.com/css2?family=Inter:wght@300;400;500;700&display=swap

Parent link : https://archibus.vodacom.co.za/_Incapsula_Resource?CWUDNSAI=23&xinfo=6-50761907-0%200NNN%20RT%281691953429171%2013568%29%20q%280%20-1%20-1%200%29%20r%280%20-1%29%20B15%284%2C200%2C0%29%20U18&incident_id=128000730324386403-257296789038699078&edet=15&cinfo=04000000&rpinfo=0&mth=GET
Found following resource links without integrity checks (only first 10 links are reported)
https://fonts.googleapis.com/css2?family=Inter:wght@300;400;500;700&display=swap

Parent link : https://archibus.vodacom.co.za/_Incapsula_Resource?CWUDNSAI=23&xinfo=8-71777546-0%200NNN%20RT%281691953415895%209146%29%20q%280%20-1%20-1%202%29%20r%280%20-1%29%20B15%284%2C200%2C0%29%20U18&incident_id=128000730324386403-355359155923456584&edet=15&cinfo=04000000&rpinfo=0&mth=GET
Found following resource links without integrity checks (only first 10 links are reported)
https://fonts.googleapis.com/css2?family=Inter:wght@300;400;500;700&display=swap
Please check there may be more pages with subresource links without integrity checks.

150202 Missing header: X-Content-Type-Options (1)

150202 Missing header: X-Content-Type-Options

archibus.vodacom.co.za/archibus

Finding #	10510599	**Severity**	Information Gathered - Level 2
Unique #	2956bce2-7150-41e1-a0d5-1ab77a63e1c2		
Group	Security Weaknesses		
CWE	CWE-16, CWE-1032	**Detection Date**	11 Feb 2024 21:02 GMT+0200
OWASP	A5 Security Misconfiguration		
WASC	WASC-15 APPLICATION MISCONFIGURATION		

Details

Threat

The X-Content-Type-Options response header is not present. WAS reports missing X-Content-Type-Options header on each crawled link for both static and dynamic responses. The scanner performs the check not only on 200 responses but 4xx and 5xx responses as well. It's also possible the QID will be reported on directory-level links.

Impact

All web browsers employ a content-sniffing algorithm that inspects the contents of HTTP responses and also occasionally overrides the MIME type provided by the server. If X-Content-Type-Options header is not present, browsers can potentially be tricked into treating non-HTML response as HTML. An attacker can then potentially leverage the functionality to perform a cross-site scripting (XSS) attack. This specific case is known as a Content-Sniffing XSS (CS-XSS) attack.

Solution

It is recommended to disable browser content sniffing by adding the X-Content-Type-Options header to the HTTP response with a value of 'nosniff'. Also, ensure that the 'Content-Type' header is set correctly on responses.

Results

X-Content-Type-Options: Header missing
Response headers on link: GET https://archibus.vodacom.co.za/favicon.ico response code: 200
cache-control: max-age=86380, public
content-length: 21630
content-security-policy-report-only: default-src 'self' 'unsafe-eval' 'unsafe-hashes' 'unsafe-inline' data: blob: ; form-action 'none' data: blob: ; report-uri /csp_report
content-type: image/x-icon
date: Sun, 11 Feb 2024 19:03:38 GMT
etag: W/"21630-1648737254000"
expires: Mon, 12 Feb 2024 19:03:18 GMT
last-modified: Thu, 31 Mar 2022 14:34:14 GMT
x-cdn: Imperva
x-iinfo: 60-17038774-0 0CNN RT(1707678198155 20620) q(0 -1 -1 -1) r(0 -1)
Set-Cookie: visid_incap_2776849=2mCPlvHbTaSKgOs2WBZQC/YZyWUAAAAAQUIPAAAAAAAWwMvjPe13zMYdphiXlTQy; HttpOnly; expires=Sun, 09-Feb-2025 22:21:11 GMT; domain=.vodacom.co.za; path=/
Set-Cookie: nlbi_2776849=ogi1WuqyhRkuEuYJZU49BAAAAABLcyLrdKjEmQdibbXYNFmh; domain=.vodacom.co.za; path=/
Set-Cookie: incap_ses_1687_2776849=9uxXXci+jlSe7PgfvG1pF/YZyWUAAAAAfr+BmEPjvWAiYHFjqA+aDQ==; domain=.vodacom.co.za; path=/

Header missing on the following link(s):
(Only first 50 such pages are listed)

GET https://archibus.vodacom.co.za/favicon.ico response code: 200
GET https://archibus.vodacom.co.za/FPRWin/index.aspx response code: 401
GET https://archibus.vodacom.co.za/Leasure-the-deed-will-the-clipt-Angely-ands-Banq response code: 200
GET https://archibus.vodacom.co.za/tomcat.css response code: 200
GET https://archibus.vodacom.co.za/docs/ response code: 404
GET https://archibus.vodacom.co.za/docs/config/ response code: 404
GET https://archibus.vodacom.co.za/examples/ response code: 404
GET https://archibus.vodacom.co.za/docs/security-howto.html response code: 404
GET https://archibus.vodacom.co.za/docs/manager-howto.html response code: 404
GET https://archibus.vodacom.co.za/docs/cluster-howto.html response code: 404
GET https://archibus.vodacom.co.za/manager/status response code: 404
GET https://archibus.vodacom.co.za/manager/html response code: 404
GET https://archibus.vodacom.co.za/host-manager/html response code: 404
GET https://archibus.vodacom.co.za/docs/setup.html response code: 404
GET https://archibus.vodacom.co.za/docs/appdev/ response code: 404
GET https://archibus.vodacom.co.za/docs/realm-howto.html response code: 404
GET https://archibus.vodacom.co.za/docs/jndi-datasource-examples-howto.html response code: 404
GET https://archibus.vodacom.co.za/docs/RELEASE-NOTES.txt response code: 404
GET https://archibus.vodacom.co.za/docs/api/index.html response code: 404
GET https://archibus.vodacom.co.za/docs/changelog.html response code: 404
GET https://archibus.vodacom.co.za/docs/deployer-howto.html response code: 404
GET https://archibus.vodacom.co.za/_Incapsula_Resource?SWJIYLWA=719d34d31c8e3a6e6fffd425f7e032f3&ns=19&cb=1246563959 response code: 200
GET https://archibus.vodacom.co.za/_Incapsula_Resource?SWJIYLWA=719d34d31c8e3a6e6fffd425f7e032f3&ns=5&cb=2085785877 response code: 200
GET https://archibus.vodacom.co.za/FPRWin/ response code: 401
GET https://archibus.vodacom.co.za/_Incapsula_Resource?SWJIYLWA=719d34d31c8e3a6e6fffd425f7e032f3%22ns=10%22cb=718590515 response code: 200
GET https://archibus.vodacom.co.za/Leasure-the-deed-will-the-clipt-Angely-ands-Banq?d=archibus.vodacom.co.za response code: 200
GET https://archibus.vodacom.co.za/_Incapsula_Resource?SWKMTFSR=1&e=0.3450785737536535 response code: 200
GET https://archibus.vodacom.co.za/_Incapsula_Resource?SWJIYLWA=719d34d31c8e3a6e6fffd425f7e032f3&ns=10&cb=718590515 response code: 200
GET https://archibus.vodacom.co.za/_Incapsula_Resource?SWJIYLWA=719d34d31c8e3a6e6fffd425f7e032f3&ns=30&cb=757409821 response code: 200
GET https://archibus.vodacom.co.za/_Incapsula_Resource?SWJIYLWA=719d34d31c8e3a6e6fffd425f7e032f3%22ns=23%22cb=682184485 response code: 200
GET https://archibus.vodacom.co.za/_Incapsula_Resource?SWKMTFSR=1&e=0.5272987180813904 response code: 200
GET https://archibus.vodacom.co.za/_Incapsula_Resource?SWJIYLWA=719d34d31c8e3a6e6fffd425f7e032f3&ns=23&cb=682184485 response code: 200
GET https://archibus.vodacom.co.za/_Incapsula_Resource?SWJIYLWA=719d34d31c8e3a6e6fffd425f7e032f3&ns=49&cb=1264811833 response code: 200
GET https://archibus.vodacom.co.za/_Incapsula_Resource?SWJIYLWA=719d34d31c8e3a6e6fffd425f7e032f3&ns=52&cb=1058230007 response code: 200
GET https://archibus.vodacom.co.za/_Incapsula_Resource?SWJIYLWA=719d34d31c8e3a6e6fffd425f7e032f3%22ns=31%22cb=292274561 response code: 200
GET https://archibus.vodacom.co.za/_Incapsula_Resource?SWJIYLWA=719d34d31c8e3a6e6fffd425f7e032f3&ns=31&cb=292274561 response code: 200
GET https://archibus.vodacom.co.za/_Incapsula_Resource?SWKMTFSR=1&e=0.8762218735550797 response code: 200
GET https://archibus.vodacom.co.za/_Incapsula_Resource?SWKMTFSR=1&e=0.20939986879542816 response code: 200
GET https://archibus.vodacom.co.za/_Incapsula_Resource?SWJIYLWA=719d34d31c8e3a6e6fffd425f7e032f3%22ns=33%22cb=462486625 response code: 200
GET https://archibus.vodacom.co.za/_Incapsula_Resource?SWKMTFSR=1&e=0.657332483118807 response code: 200
GET https://archibus.vodacom.co.za/_Incapsula_Resource?SWJIYLWA=719d34d31c8e3a6e6fffd425f7e032f3%22ns=40%22cb=1925770764 response code: 200
GET https://archibus.vodacom.co.za/_Incapsula_Resource?SWJIYLWA=719d34d31c8e3a6e6fffd425f7e032f3%22ns=57%22cb=149715920 response code: 200
GET https://archibus.vodacom.co.za/_Incapsula_Resource?SWKMTFSR=1&e=0.9411161046872494 response code: 200
GET https://archibus.vodacom.co.za/_Incapsula_Resource?SWJIYLWA=719d34d31c8e3a6e6fffd425f7e032f3%22ns=62%22cb=759071798 response code: 200
GET https://archibus.vodacom.co.za/manager/ response code: 404
GET https://archibus.vodacom.co.za/_Incapsula_Resource?SWJIYLWA=719d34d31c8e3a6e6fffd425f7e032f3%22ns=63%22cb=261016948 response code: 200
GET https://archibus.vodacom.co.za/_Incapsula_Resource?SWKMTFSR=1&e=0.10408580974368586 response code: 200
GET https://archibus.vodacom.co.za/_Incapsula_Resource?SWKMTFSR=1&e=0.748959364503075 response code: 200
GET https://archibus.vodacom.co.za/host-manager/ response code: 404
GET https://archibus.vodacom.co.za/docs/api/ response code: 404

WAS Web Application Report

150206 Content-Security-Policy Not Implemented (1)

150206 Content-Security-Policy Not Implemented — *archibus.vodacom.co.za/archibus*

Finding #	10510602	**Severity**	Information Gathered - Level 2
Unique #	8bc9da76-e0de-4e15-9143-3240acdd2948		
Group	Security Weaknesses		
CWE	CWE-16, CWE-1032	**Detection Date**	11 Feb 2024 21:02 GMT+0200
OWASP	A5 Security Misconfiguration		
WASC	WASC-15 APPLICATION MISCONFIGURATION		

Details

Threat

No Content-Security-Policy (CSP) is specified for the page. WAS checks for the missing CSP on all static and dynamic pages. It checks for CSP in the response headers (Content-Security-Policy, X-Content-Security-Policy or X-Webkit-CSP) and in response body (http-equiv="Content-Security-Policy" meta tag).

HTTP 4xx and 5xx responses can also be susceptible to attacks such as XSS. For better security it's important to set appropriate CSP policies on 4xx and 5xx responses as well.

Impact

Content-Security Policy is a defense mechanism that can significantly reduce the risk and impact of XSS attacks in modern browsers. The CSP specification provides a set of content restrictions for web resources and a mechanism for transmitting the policy from a server to a client where the policy is enforced. When a Content Security Policy is specified, a number of default behaviors in user agents are changed; specifically inline content and JavaScript eval constructs are not interpreted without additional directives. In short, CSP allows you to create a whitelist of sources of the trusted content. The CSP policy instructs the browser to only render resources from those whitelisted sources. Even though an attacker can find a security vulnerability in the application through which to inject script, the script won't match the whitelisted sources defined in the CSP policy, and therefore will not be executed.

The absence of Content Security Policy in the response will allow the attacker to exploit vulnerabilities as the protection provided by the browser is not at all leveraged by the Web application. If secure CSP configuration is not implemented, browsers will not be able to block content-injection attacks such as Cross-Site Scripting and Clickjacking.

Solution

Appropriate CSP policies help prevent content-injection attacks such as cross-site scripting (XSS) and clickjacking. It's recommended to add secure CSP policies as a part of a defense-in-depth approach for securing web applications.

References:
- https://cheatsheetseries.owasp.org/cheatsheets/Content_Security_Policy_Cheat_Sheet.html
- https://developers.google.com/web/fundamentals/security/csp/

Results

Content-Security-Policy: Header missing
Response headers on link: GET https://archibus.vodacom.co.za/favicon.ico response code: 200
cache-control: max-age=86380, public
content-length: 21630
content-security-policy-report-only: default-src 'self' 'unsafe-eval' 'unsafe-hashes' 'unsafe-inline' data: blob: ; form-action 'none' data: blob: ; report-uri /csp_report
content-type: image/x-icon
date: Sun, 11 Feb 2024 19:03:38 GMT
etag: W/"21630-1648737254000"
expires: Mon, 12 Feb 2024 19:03:18 GMT
last-modified: Thu, 31 Mar 2022 14:34:14 GMT
x-cdn: Imperva
x-iinfo: 60-17038774-0 0CNN RT(1707678198155 20620) q(0 -1 -1 -1) r(0 -1)
Set-Cookie: visid_incap_2776849=2mCPlvHbTaSKgOs2WBZQC/YZyWUAAAAAQUIPAAAAAAAWwMvjPe13zMYdphiXlTQy; HttpOnly; expires=Sun, 09-Feb-2025 22:21:11 GMT; domain=.vodacom.co.za; path=/
Set-Cookie: nlbi_2776849=ogi1WuqyhRkuEuYJZU49BAAAAABLcyLrdKjEmQdibbXYNFmh; domain=.vodacom.co.za; path=/
Set-Cookie: incap_ses_1687_2776849=9uxXXci+jlSe7PgfvG1pF/YZyWUAAAAAfr+BmEPjvWAiYHFjqA+aDQ==; domain=.vodacom.co.za; path=/

Header missing, but Content-Security-Policy-Report-Only header found. It allows for testing different directives to determine how the current policy can be trimmed or modified to create the most restrictive policy possible, however still allowing all required resources. CSP header missing on the link: GET https://archibus.vodacom.co.za/favicon.ico response code: 200

Content-Security-Policy: Header missing, but Content-Security-Policy-Report-Only header found. It allows for testing different directives to determine how the current policy can be trimmed or

modified to create the most restrictive policy possible, however still allowing all required resources. CSP header missing on the link: GET https://archibus.vodacom.co.za/FPRWin/index.aspx response code: 401

Content-Security-Policy: Header missing, but Content-Security-Policy-Report-Only header found. It allows for testing different directives to determine how the current policy can be trimmed or modified to create the most restrictive policy possible, however still allowing all required resources. CSP header missing on the link: GET https://archibus.vodacom.co.za/Leasure-the-deed-will-the-clipt-Angely-ands-Banq response code: 200

Content-Security-Policy: Header missing, but Content-Security-Policy-Report-Only header found. It allows for testing different directives to determine how the current policy can be trimmed or modified to create the most restrictive policy possible, however still allowing all required resources. CSP header missing on the link: GET https://archibus.vodacom.co.za/tomcat.css response code: 200

Content-Security-Policy: Header missing, but Content-Security-Policy-Report-Only header found. It allows for testing different directives to determine how the current policy can be trimmed or modified to create the most restrictive policy possible, however still allowing all required resources. CSP header missing on the link: GET https://archibus.vodacom.co.za/docs/ response code: 404

Content-Security-Policy: Header missing, but Content-Security-Policy-Report-Only header found. It allows for testing different directives to determine how the current policy can be trimmed or modified to create the most restrictive policy possible, however still allowing all required resources. CSP header missing on the link: GET https://archibus.vodacom.co.za/docs/config/ response code: 404

Content-Security-Policy: Header missing, but Content-Security-Policy-Report-Only header found. It allows for testing different directives to determine how the current policy can be trimmed or modified to create the most restrictive policy possible, however still allowing all required resources. CSP header missing on the link: GET https://archibus.vodacom.co.za/examples/ response code: 404

Content-Security-Policy: Header missing, but Content-Security-Policy-Report-Only header found. It allows for testing different directives to determine how the current policy can be trimmed or modified to create the most restrictive policy possible, however still allowing all required resources. CSP header missing on the link: GET https://archibus.vodacom.co.za/docs/security-howto.html response code: 404

Content-Security-Policy: Header missing, but Content-Security-Policy-Report-Only header found. It allows for testing different directives to determine how the current policy can be trimmed or modified to create the most restrictive policy possible, however still allowing all required resources. CSP header missing on the link: GET https://archibus.vodacom.co.za/docs/manager-howto.html response code: 404

Content-Security-Policy: Header missing, but Content-Security-Policy-Report-Only header found. It allows for testing different directives to determine how the current policy can be trimmed or modified to create the most restrictive policy possible, however still allowing all required resources. CSP header missing on the link: GET https://archibus.vodacom.co.za/docs/cluster-howto.html response code: 404

Content-Security-Policy: Header missing, but Content-Security-Policy-Report-Only header found. It allows for testing different directives to determine how the current policy can be trimmed or modified to create the most restrictive policy possible, however still allowing all required resources. CSP header missing on the link: GET https://archibus.vodacom.co.za/manager/status response code: 404

Content-Security-Policy: Header missing, but Content-Security-Policy-Report-Only header found. It allows for testing different directives to determine how the current policy can be trimmed or modified to create the most restrictive policy possible, however still allowing all required resources. CSP header missing on the link: GET https://archibus.vodacom.co.za/manager/html response code: 404

Content-Security-Policy: Header missing, but Content-Security-Policy-Report-Only header found. It allows for testing different directives to determine how the current policy can be trimmed or modified to create the most restrictive policy possible, however still allowing all required resources. CSP header missing on the link: GET https://archibus.vodacom.co.za/host-manager/html response code: 404

Content-Security-Policy: Header missing, but Content-Security-Policy-Report-Only header found. It allows for testing different directives to determine how the current policy can be trimmed or modified to create the most restrictive policy possible, however still allowing all required resources. CSP header missing on the link: GET https://archibus.vodacom.co.za/docs/setup.html response code: 404

Content-Security-Policy: Header missing, but Content-Security-Policy-Report-Only header found. It allows for testing different directives to determine how the current policy can be trimmed or modified to create the most restrictive policy possible, however still allowing all required resources. CSP header missing on the link: GET https://archibus.vodacom.co.za/docs/appdev/ response code: 404

Content-Security-Policy: Header missing, but Content-Security-Policy-Report-Only header found. It allows for testing different directives to determine how the current policy can be trimmed or modified to create the most restrictive policy possible, however still allowing all required resources. CSP header missing on the link: GET https://archibus.vodacom.co.za/docs/realm-howto.html response code: 404

Content-Security-Policy: Header missing, but Content-Security-Policy-Report-Only header found. It allows for testing different directives to determine how the current policy can be trimmed or modified to create the most restrictive policy possible, however still allowing all required resources. CSP header missing on the link: GET https://archibus.vodacom.co.za/docs/jndi-datasource-examples-howto.html response code: 404

Content-Security-Policy: Header missing, but Content-Security-Policy-Report-Only header found. It allows for testing different directives to determine how the current policy can be trimmed or modified to create the most restrictive policy possible, however still allowing all required resources. CSP header missing on the link: GET https://archibus.vodacom.co.za/docs/RELEASE-NOTES.txt response code: 404

Content-Security-Policy: Header missing, but Content-Security-Policy-Report-Only header found. It allows for testing different directives to determine how the current policy can be trimmed or modified to create the most restrictive policy possible, however still allowing all required resources. CSP header missing on the link: GET https://archibus.vodacom.co.za/docs/api/index.html response code: 404

Content-Security-Policy: Header missing, but Content-Security-Policy-Report-Only header found. It allows for testing different directives to determine how the current policy can be trimmed or modified to create the most restrictive policy possible, however still allowing all required resources. CSP header missing on the link: GET https://archibus.vodacom.co.za/docs/changelog.html response code: 404

Content-Security-Policy: Header missing, but Content-Security-Policy-Report-Only header found. It allows for testing different directives to determine how the current policy can be trimmed or modified to create the most restrictive policy possible, however still allowing all required resources. CSP header missing on the link: GET https://archibus.vodacom.co.za/docs/deployer-howto.html response code: 404

Content-Security-Policy: Header missing, but Content-Security-Policy-Report-Only header found. It allows for testing different directives to determine how the current policy can be trimmed or modified to create the most restrictive policy possible, however still allowing all required resources. CSP header missing on the link: GET https://archibus.vodacom.co.za/_Incapsula_Resource?SWJIYLWA=719d34d31c8e3a6e6fffd425f7e032f3&ns=19&cb=1246563959 response code: 200

Content-Security-Policy: Header missing, but Content-Security-Policy-Report-Only header found. It allows for testing different directives to determine how the current policy can be trimmed or modified to create the most restrictive policy possible, however still allowing all required resources. CSP header missing on the link: GET https://archibus.vodacom.co.za/_Incapsula_Resource?SWJIYLWA=719d34d31c8e3a6e6fffd425f7e032f3&ns=5&cb=2085785877 response code: 200

Content-Security-Policy: Header missing, but Content-Security-Policy-Report-Only header found. It allows for testing different directives to determine how the current policy can be trimmed or

modified to create the most restrictive policy possible, however still allowing all required resources. CSP header missing on the link: GET https://archibus.vodacom.co.za/FPRWin/ response code: 401

Content-Security-Policy: Header missing, but Content-Security-Policy-Report-Only header found. It allows for testing different directives to determine how the current policy can be trimmed or modified to create the most restrictive policy possible, however still allowing all required resources. CSP header missing on the link: GET https://archibus.vodacom.co.za/_Incapsula_Resource?SWJIYLWA=719d34d31c8e3a6e6fffd425f7e032f3%22ns=10%22cb=718590515 response code: 200

Content-Security-Policy: Header missing, but Content-Security-Policy-Report-Only header found. It allows for testing different directives to determine how the current policy can be trimmed or modified to create the most restrictive policy possible, however still allowing all required resources. CSP header missing on the link: GET https://archibus.vodacom.co.za/Leasure-the-deed-will-the-clipt-Angely-ands-Banq?d=archibus.vodacom.co.za response code: 200

Content-Security-Policy: Header missing, but Content-Security-Policy-Report-Only header found. It allows for testing different directives to determine how the current policy can be trimmed or modified to create the most restrictive policy possible, however still allowing all required resources. CSP header missing on the link: GET https://archibus.vodacom.co.za/_Incapsula_Resource?SWKMTFSR=1&e=0.3450785737536535 response code: 200

Content-Security-Policy: Header missing, but Content-Security-Policy-Report-Only header found. It allows for testing different directives to determine how the current policy can be trimmed or modified to create the most restrictive policy possible, however still allowing all required resources. CSP header missing on the link: GET https://archibus.vodacom.co.za/_Incapsula_Resource?SWJIYLWA=719d34d31c8e3a6e6fffd425f7e032f3&ns=10&cb=718590515 response code: 200

Content-Security-Policy: Header missing, but Content-Security-Policy-Report-Only header found. It allows for testing different directives to determine how the current policy can be trimmed or modified to create the most restrictive policy possible, however still allowing all required resources. CSP header missing on the link: GET https://archibus.vodacom.co.za/_Incapsula_Resource?SWJIYLWA=719d34d31c8e3a6e6fffd425f7e032f3&ns=30&cb=757409821 response code: 200

Content-Security-Policy: Header missing, but Content-Security-Policy-Report-Only header found. It allows for testing different directives to determine how the current policy can be trimmed or modified to create the most restrictive policy possible, however still allowing all required resources. CSP header missing on the link: GET https://archibus.vodacom.co.za/_Incapsula_Resource?SWJIYLWA=719d34d31c8e3a6e6fffd425f7e032f3%22ns=23%22cb=682184485 response code: 200

Content-Security-Policy: Header missing, but Content-Security-Policy-Report-Only header found. It allows for testing different directives to determine how the current policy can be trimmed or modified to create the most restrictive policy possible, however still allowing all required resources. CSP header missing on the link: GET https://archibus.vodacom.co.za/_Incapsula_Resource?SWKMTFSR=1&e=0.5272987180813904 response code: 200

Content-Security-Policy: Header missing, but Content-Security-Policy-Report-Only header found. It allows for testing different directives to determine how the current policy can be trimmed or modified to create the most restrictive policy possible, however still allowing all required resources. CSP header missing on the link: GET https://archibus.vodacom.co.za/_Incapsula_Resource?SWJIYLWA=719d34d31c8e3a6e6fffd425f7e032f3&ns=23&cb=682184485 response code: 200

Content-Security-Policy: Header missing, but Content-Security-Policy-Report-Only header found. It allows for testing different directives to determine how the current policy can be trimmed or modified to create the most restrictive policy possible, however still allowing all required resources. CSP header missing on the link: GET https://archibus.vodacom.co.za/_Incapsula_Resource?SWJIYLWA=719d34d31c8e3a6e6fffd425f7e032f3&ns=49&cb=1264811833 response code: 200

Content-Security-Policy: Header missing, but Content-Security-Policy-Report-Only header found. It allows for testing different directives to determine how the current policy can be trimmed or modified to create the most restrictive policy possible, however still allowing all required resources. CSP header missing on the link: GET https://archibus.vodacom.co.za/_Incapsula_Resource?SWJIYLWA=719d34d31c8e3a6e6fffd425f7e032f3&ns=52&cb=1058230007 response code: 200

Content-Security-Policy: Header missing, but Content-Security-Policy-Report-Only header found. It allows for testing different directives to determine how the current policy can be trimmed or modified to create the most restrictive policy possible, however still allowing all required resources. CSP header missing on the link: GET https://archibus.vodacom.co.za/_Incapsula_Resource?SWJIYLWA=719d34d31c8e3a6e6fffd425f7e032f3%22ns=31%22cb=292274561 response code: 200

Content-Security-Policy: Header missing, but Content-Security-Policy-Report-Only header found. It allows for testing different directives to determine how the current policy can be trimmed or modified to create the most restrictive policy possible, however still allowing all required resources. CSP header missing on the link: GET https://archibus.vodacom.co.za/_Incapsula_Resource?SWJIYLWA=719d34d31c8e3a6e6fffd425f7e032f3&ns=31&cb=292274561 response code: 200

Content-Security-Policy: Header missing, but Content-Security-Policy-Report-Only header found. It allows for testing different directives to determine how the current policy can be trimmed or modified to create the most restrictive policy possible, however still allowing all required resources. CSP header missing on the link: GET https://archibus.vodacom.co.za/_Incapsula_Resource?SWKMTFSR=1&e=0.8762218735550797 response code: 200

Content-Security-Policy: Header missing, but Content-Security-Policy-Report-Only header found. It allows for testing different directives to determine how the current policy can be trimmed or modified to create the most restrictive policy possible, however still allowing all required resources. CSP header missing on the link: GET https://archibus.vodacom.co.za/_Incapsula_Resource?SWKMTFSR=1&e=0.20939986879542816 response code: 200

Content-Security-Policy: Header missing, but Content-Security-Policy-Report-Only header found. It allows for testing different directives to determine how the current policy can be trimmed or modified to create the most restrictive policy possible, however still allowing all required resources. CSP header missing on the link: GET https://archibus.vodacom.co.za/_Incapsula_Resource?SWJIYLWA=719d34d31c8e3a6e6fffd425f7e032f3%22ns=33%22cb=462486625 response code: 200

Content-Security-Policy: Header missing, but Content-Security-Policy-Report-Only header found. It allows for testing different directives to determine how the current policy can be trimmed or modified to create the most restrictive policy possible, however still allowing all required resources. CSP header missing on the link: GET https://archibus.vodacom.co.za/_Incapsula_Resource?SWKMTFSR=1&e=0.657332483118807 response code: 200

Content-Security-Policy: Header missing, but Content-Security-Policy-Report-Only header found. It allows for testing different directives to determine how the current policy can be trimmed or modified to create the most restrictive policy possible, however still allowing all required resources. CSP header missing on the link: GET https://archibus.vodacom.co.za/_Incapsula_Resource?SWJIYLWA=719d34d31c8e3a6e6fffd425f7e032f3%22ns=40%22cb=1925770764 response code: 200

Content-Security-Policy: Header missing, but Content-Security-Policy-Report-Only header found. It allows for testing different directives to determine how the current policy can be trimmed or modified to create the most restrictive policy possible, however still allowing all required resources. CSP header missing on the link: GET https://archibus.vodacom.co.za/_Incapsula_Resource?SWJIYLWA=719d34d31c8e3a6e6fffd425f7e032f3%22ns=57%22cb=149715920 response code: 200

Content-Security-Policy: Header missing, but Content-Security-Policy-Report-Only header found. It allows for testing different directives to determine how the current policy can be trimmed or modified to create the most restrictive policy possible, however still allowing all required resources. CSP header missing on the link: GET https://archibus.vodacom.co.za/_Incapsula_Resource?SWKMTFSR=1&e=0.9411161046872494 response code: 200

Content-Security-Policy: Header missing, but Content-Security-Policy-Report-Only header found. It allows for testing different directives to determine how the current policy can be trimmed or modified to create the most restrictive policy possible, however still allowing all required resources. CSP header missing on the link: GET https://archibus.vodacom.co.za/_Incapsula_Resource?SWJIYLWA=719d34d31c8e3a6e6fffd425f7e032f3%22ns=62%22cb=759071798 response code: 200

Content-Security-Policy: Header missing, but Content-Security-Policy-Report-Only header found. It allows for testing different directives to determine how the current policy can be trimmed or modified to create the most restrictive policy possible, however still allowing all required resources. CSP header missing on the link: GET https://archibus.vodacom.co.za/manager/ response code: 404

Content-Security-Policy: Header missing, but Content-Security-Policy-Report-Only header found. It allows for testing different directives to determine how the current policy can be trimmed or modified to create the most restrictive policy possible, however still allowing all required resources. CSP header missing on the link: GET https://archibus.vodacom.co.za/_Incapsula_Resource?SWJIYLWA=719d34d31c8e3a6e6fffd425f7e032f3%22ns=63%22cb=261016948 response code: 200

Content-Security-Policy: Header missing, but Content-Security-Policy-Report-Only header found. It allows for testing different directives to determine how the current policy can be trimmed or modified to create the most restrictive policy possible, however still allowing all required resources. CSP header missing on the link: GET https://archibus.vodacom.co.za/_Incapsula_Resource?SWKMTFSR=1&e=0.10408580974368586 response code: 200

Content-Security-Policy: Header missing, but Content-Security-Policy-Report-Only header found. It allows for testing different directives to determine how the current policy can be trimmed or modified to create the most restrictive policy possible, however still allowing all required resources. CSP header missing on the link: GET https://archibus.vodacom.co.za/_Incapsula_Resource?SWKMTFSR=1&e=0.748959364503075 response code: 200

Content-Security-Policy: Header missing, but Content-Security-Policy-Report-Only header found. It allows for testing different directives to determine how the current policy can be trimmed or modified to create the most restrictive policy possible, however still allowing all required resources. CSP header missing on the link: GET https://archibus.vodacom.co.za/host-manager/ response code: 404

Content-Security-Policy: Header missing, but Content-Security-Policy-Report-Only header found. It allows for testing different directives to determine how the current policy can be trimmed or modified to create the most restrictive policy possible, however still allowing all required resources. CSP header missing on the link: GET https://archibus.vodacom.co.za/docs/api/ response code: 404

150208 Missing header: Referrer-Policy (1)

150208 Missing header: Referrer-Policy

archibus.vodacom.co.za/archibus

Finding #	10510582	**Severity**	Information Gathered - Level 2
Unique #	05ced3bc-572b-41c5-b3c6-4809f346f6a2		
Group	Security Weaknesses		
CWE	CWE-16, CWE-1032	**Detection Date**	11 Feb 2024 21:02 GMT+0200
OWASP	A5 Security Misconfiguration		
WASC	WASC-15 APPLICATION MISCONFIGURATION		

Details

Threat

No Referrer Policy is specified for the link. WAS checks for the missing Referrer Policy on all static and dynamic pages. It checks for one of the following Referrer Policy in the response headers:

1) no-referrer
2) no-referrer-when-downgrade
3) same-origin
4) origin
5) origin-when-cross-origin
6) strict-origin
7) strict-origin-when-cross-origin

If the Referrer Policy header is not found , WAS checks in response body for meta tag containing tag name as "referrer" and one of the above Referrer Policy.

Impact

The Referrer-Policy header controls how much referrer information is sent to a site when navigating to it. Absence of Referrer-Policy header can lead to leakage of sensitive information via the referrer header.

Solution

Referrer Policy header improves security by ensuring websites don't leak sensitive information via the referrer header. It's recommended to add secure Referrer Policies as a part of a defense-in-depth approach.

References:
- https://www.w3.org/TR/referrer-policy/
- https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/Referrer-Policy

Results

Referrer-Policy: Header missing

Response headers on link: GET https://archibus.vodacom.co.za/favicon.ico response code: 200
cache-control: max-age=86380, public
content-length: 21630
content-security-policy-report-only: default-src 'self' 'unsafe-eval' 'unsafe-hashes' 'unsafe-inline' data: blob: ; form-action 'none' data: blob: ; report-uri /csp_report
content-type: image/x-icon
date: Sun, 11 Feb 2024 19:03:38 GMT
etag: W/"21630-1648737254000"
expires: Mon, 12 Feb 2024 19:03:18 GMT
last-modified: Thu, 31 Mar 2022 14:34:14 GMT
x-cdn: Imperva
x-iinfo: 60-17038774-0 0CNN RT(1707678198155 20620) q(0 -1 -1 -1) r(0 -1)
Set-Cookie: visid_incap_2776849=2mCPlvHbTaSKgOs2WBZQC/YZyWUAAAAAQUIPAAAAAAAWwMvjPe13zMYdphiXlTQy; HttpOnly; expires=Sun, 09-Feb-2025 22:21:11 GMT; domain=.vodacom.co.za; path=/
Set-Cookie: nlbi_2776849=ogi1WuqyhRkuEuYJZU49BAAAAABLcyLrdKjEmQdibbXYNFmh; domain=.vodacom.co.za; path=/
Set-Cookie: incap_ses_1687_2776849=9uxXXci+jlSe7PgfvG1pF/YZyWUAAAAAfr+BmEPjvWAiYHFjqA+aDQ==; domain=.vodacom.co.za; path=/

Header missing on the following link(s):
(Only first 50 such pages are listed)

GET https://archibus.vodacom.co.za/favicon.ico response code: 200
GET https://archibus.vodacom.co.za/FPRWin/index.aspx response code: 401
GET https://archibus.vodacom.co.za/Leasure-the-deed-will-the-clipt-Angely-ands-Banq response code: 200
GET https://archibus.vodacom.co.za/tomcat.css response code: 200
GET https://archibus.vodacom.co.za/docs/ response code: 404
GET https://archibus.vodacom.co.za/docs/config/ response code: 404
GET https://archibus.vodacom.co.za/examples/ response code: 404
GET https://archibus.vodacom.co.za/docs/security-howto.html response code: 404
GET https://archibus.vodacom.co.za/docs/manager-howto.html response code: 404
GET https://archibus.vodacom.co.za/docs/cluster-howto.html response code: 404
GET https://archibus.vodacom.co.za/manager/status response code: 404
GET https://archibus.vodacom.co.za/manager/html response code: 404
GET https://archibus.vodacom.co.za/host-manager/html response code: 404
GET https://archibus.vodacom.co.za/docs/setup.html response code: 404
GET https://archibus.vodacom.co.za/docs/appdev/ response code: 404
GET https://archibus.vodacom.co.za/docs/realm-howto.html response code: 404
GET https://archibus.vodacom.co.za/docs/jndi-datasource-examples-howto.html response code: 404
GET https://archibus.vodacom.co.za/docs/RELEASE-NOTES.txt response code: 404
GET https://archibus.vodacom.co.za/docs/api/index.html response code: 404
GET https://archibus.vodacom.co.za/docs/changelog.html response code: 404
GET https://archibus.vodacom.co.za/docs/deployer-howto.html response code: 404
GET https://archibus.vodacom.co.za/_Incapsula_Resource?SWJIYLWA=719d34d31c8e3a6e6fffd425f7e032f3&ns=19&cb=1246563959 response code: 200
GET https://archibus.vodacom.co.za/_Incapsula_Resource?SWJIYLWA=719d34d31c8e3a6e6fffd425f7e032f3&ns=5&cb=2085785877 response code: 200
GET https://archibus.vodacom.co.za/FPRWin/ response code: 401
GET https://archibus.vodacom.co.za/_Incapsula_Resource?SWJIYLWA=719d34d31c8e3a6e6fffd425f7e032f3%22ns=10%22cb=718590515 response code: 200
GET https://archibus.vodacom.co.za/Leasure-the-deed-will-the-clipt-Angely-ands-Banq?d=archibus.vodacom.co.za response code: 200
GET https://archibus.vodacom.co.za/_Incapsula_Resource?SWKMTFSR=1&e=0.3450785737536535 response code: 200
GET https://archibus.vodacom.co.za/_Incapsula_Resource?SWJIYLWA=719d34d31c8e3a6e6fffd425f7e032f3&ns=10&cb=718590515 response code: 200
GET https://archibus.vodacom.co.za/_Incapsula_Resource?SWJIYLWA=719d34d31c8e3a6e6fffd425f7e032f3&ns=30&cb=757409821 response code: 200
GET https://archibus.vodacom.co.za/_Incapsula_Resource?SWJIYLWA=719d34d31c8e3a6e6fffd425f7e032f3%22ns=23%22cb=682184485 response code: 200
GET https://archibus.vodacom.co.za/_Incapsula_Resource?SWKMTFSR=1&e=0.5272987180813904 response code: 200
GET https://archibus.vodacom.co.za/_Incapsula_Resource?SWJIYLWA=719d34d31c8e3a6e6fffd425f7e032f3&ns=23&cb=682184485 response code: 200
GET https://archibus.vodacom.co.za/_Incapsula_Resource?SWJIYLWA=719d34d31c8e3a6e6fffd425f7e032f3&ns=49&cb=1264811833 response code: 200
GET https://archibus.vodacom.co.za/_Incapsula_Resource?SWJIYLWA=719d34d31c8e3a6e6fffd425f7e032f3&ns=52&cb=1058230007 response code: 200
GET https://archibus.vodacom.co.za/_Incapsula_Resource?SWJIYLWA=719d34d31c8e3a6e6fffd425f7e032f3%22ns=31%22cb=292274561 response code: 200
GET https://archibus.vodacom.co.za/_Incapsula_Resource?SWJIYLWA=719d34d31c8e3a6e6fffd425f7e032f3&ns=31&cb=292274561 response code: 200
GET https://archibus.vodacom.co.za/_Incapsula_Resource?SWKMTFSR=1&e=0.8762218735550797 response code: 200
GET https://archibus.vodacom.co.za/_Incapsula_Resource?SWKMTFSR=1&e=0.20939986879542816 response code: 200
GET https://archibus.vodacom.co.za/_Incapsula_Resource?SWJIYLWA=719d34d31c8e3a6e6fffd425f7e032f3%22ns=33%22cb=462486625 response code: 200
GET https://archibus.vodacom.co.za/_Incapsula_Resource?SWKMTFSR=1&e=0.657332483118807 response code: 200
GET https://archibus.vodacom.co.za/_Incapsula_Resource?SWJIYLWA=719d34d31c8e3a6e6fffd425f7e032f3%22ns=40%22cb=1925770764 response code: 200
GET https://archibus.vodacom.co.za/_Incapsula_Resource?SWJIYLWA=719d34d31c8e3a6e6fffd425f7e032f3%22ns=57%22cb=149715920 response code: 200
GET https://archibus.vodacom.co.za/_Incapsula_Resource?SWKMTFSR=1&e=0.9411161046872494 response code: 200
GET https://archibus.vodacom.co.za/_Incapsula_Resource?SWJIYLWA=719d34d31c8e3a6e6fffd425f7e032f3%22ns=62%22cb=759071798 response code: 200
GET https://archibus.vodacom.co.za/manager/ response code: 404
GET https://archibus.vodacom.co.za/_Incapsula_Resource?SWJIYLWA=719d34d31c8e3a6e6fffd425f7e032f3%22ns=63%22cb=261016948 response code: 200
GET https://archibus.vodacom.co.za/_Incapsula_Resource?SWKMTFSR=1&e=0.10408580974368586 response code: 200
GET https://archibus.vodacom.co.za/_Incapsula_Resource?SWKMTFSR=1&e=0.748959364503075 response code: 200
GET https://archibus.vodacom.co.za/host-manager/ response code: 404
GET https://archibus.vodacom.co.za/docs/api/ response code: 404

150248 Missing header: Permissions-Policy (1)

150248 Missing header: Permissions-Policy *archibus.vodacom.co.za/archibus*

Finding #	10510590	**Severity**	Information Gathered - Level 2
Unique #	520c91ce-8ef6-4910-97b5-12cbba26fc56		
Group	Security Weaknesses		
CWE	CWE-284	**Detection Date**	11 Feb 2024 21:02 GMT+0200
OWASP	A5 Security Misconfiguration		

WAS Web Application Report

WASC -

Details

Threat
The Permissions-Policy response header is not present.

Impact
Permissions-Policy allows web developers to selectively enable, disable, or modify the behavior of some of the browser features and APIs within their application.

A user agent has a set of supported features(Policy Controlled Features), which is the set of features which it allows to be controlled through policies.

Not defining policy for unused and risky policy controlled features may leave application vulnerable.

Solution
It is recommended to define policy for policy controlled features to make application more secure.

References:
Permissions-Policy W3C Working Draft
Policy Controlled Features

Results

Permissions-Policy: Header missing
Response headers on link: GET https://archibus.vodacom.co.za/favicon.ico response code: 200
cache-control: max-age=86380, public
content-length: 21630
content-security-policy-report-only: default-src 'self' 'unsafe-eval' 'unsafe-hashes' 'unsafe-inline' data: blob: ; form-action 'none' data: blob: ; report-uri /csp_report
content-type: image/x-icon
date: Sun, 11 Feb 2024 19:03:38 GMT
etag: W/"21630-1648737254000"
expires: Mon, 12 Feb 2024 19:03:18 GMT
last-modified: Thu, 31 Mar 2022 14:34:14 GMT
x-cdn: Imperva
x-iinfo: 60-17038774-0 0CNN RT(1707678198155 20620) q(0 -1 -1 -1) r(0 -1)
Set-Cookie: visid_incap_2776849=2mCPlvHbTaSKgOs2WBZQC/YZyWUAAAAAQUIPAAAAAAAWwMvjPe13zMYdphiXlTQy; HttpOnly; expires=Sun, 09-Feb-2025 22:21:11 GMT; domain=.vodacom.co.za; path=/
Set-Cookie: nlbi_2776849=ogi1WuqyhRkuEuYJZU49BAAAAABLcyLrdKjEmQdibbXYNFmh; domain=.vodacom.co.za; path=/
Set-Cookie: incap_ses_1687_2776849=9uxXXci+jlSe7PgfvG1pF/YZyWUAAAAAfr+BmEPjvWAiYHFjqA+aDQ==; domain=.vodacom.co.za; path=/

Header missing on the following link(s):
(Only first 50 such pages are listed)

GET https://archibus.vodacom.co.za/favicon.ico response code: 200
GET https://archibus.vodacom.co.za/FPRWin/index.aspx response code: 401
GET https://archibus.vodacom.co.za/Leasure-the-deed-will-the-clipt-Angely-ands-Banq response code: 200
GET https://archibus.vodacom.co.za/tomcat.css response code: 200
GET https://archibus.vodacom.co.za/docs/ response code: 404
GET https://archibus.vodacom.co.za/docs/config/ response code: 404
GET https://archibus.vodacom.co.za/examples/ response code: 404
GET https://archibus.vodacom.co.za/docs/security-howto.html response code: 404
GET https://archibus.vodacom.co.za/docs/manager-howto.html response code: 404
GET https://archibus.vodacom.co.za/docs/cluster-howto.html response code: 404
GET https://archibus.vodacom.co.za/manager/status response code: 404
GET https://archibus.vodacom.co.za/manager/html response code: 404
GET https://archibus.vodacom.co.za/host-manager/html response code: 404
GET https://archibus.vodacom.co.za/docs/setup.html response code: 404
GET https://archibus.vodacom.co.za/docs/appdev/ response code: 404
GET https://archibus.vodacom.co.za/docs/realm-howto.html response code: 404
GET https://archibus.vodacom.co.za/docs/jndi-datasource-examples-howto.html response code: 404
GET https://archibus.vodacom.co.za/docs/RELEASE-NOTES.txt response code: 404
GET https://archibus.vodacom.co.za/docs/api/index.html response code: 404
GET https://archibus.vodacom.co.za/docs/changelog.html response code: 404
GET https://archibus.vodacom.co.za/docs/deployer-howto.html response code: 404
GET https://archibus.vodacom.co.za/_Incapsula_Resource?SWJIYLWA=719d34d31c8e3a6e6fffd425f7e032f3&ns=19&cb=1246563959 response code: 200
GET https://archibus.vodacom.co.za/_Incapsula_Resource?SWJIYLWA=719d34d31c8e3a6e6fffd425f7e032f3&ns=5&cb=2085785877 response code: 200
GET https://archibus.vodacom.co.za/FPRWin/ response code: 401

GET https://archibus.vodacom.co.za/_Incapsula_Resource?SWJIYLWA=719d34d31c8e3a6e6fffd425f7e032f3%22ns=10%22cb=718590515 response code: 200
GET https://archibus.vodacom.co.za/Leasure-the-deed-will-the-clipt-Angely-ands-Banq?d=archibus.vodacom.co.za response code: 200
GET https://archibus.vodacom.co.za/_Incapsula_Resource?SWKMTFSR=1&e=0.3450785737536535 response code: 200
GET https://archibus.vodacom.co.za/_Incapsula_Resource?SWJIYLWA=719d34d31c8e3a6e6fffd425f7e032f3&ns=10&cb=718590515 response code: 200
GET https://archibus.vodacom.co.za/_Incapsula_Resource?SWJIYLWA=719d34d31c8e3a6e6fffd425f7e032f3&ns=30&cb=757409821 response code: 200
GET https://archibus.vodacom.co.za/_Incapsula_Resource?SWJIYLWA=719d34d31c8e3a6e6fffd425f7e032f3%22ns=23%22cb=682184485 response code: 200
GET https://archibus.vodacom.co.za/_Incapsula_Resource?SWKMTFSR=1&e=0.5272987180813904 response code: 200
GET https://archibus.vodacom.co.za/_Incapsula_Resource?SWJIYLWA=719d34d31c8e3a6e6fffd425f7e032f3&ns=23&cb=682184485 response code: 200
GET https://archibus.vodacom.co.za/_Incapsula_Resource?SWJIYLWA=719d34d31c8e3a6e6fffd425f7e032f3&ns=49&cb=1264811833 response code: 200
GET https://archibus.vodacom.co.za/_Incapsula_Resource?SWJIYLWA=719d34d31c8e3a6e6fffd425f7e032f3&ns=52&cb=1058230007 response code: 200
GET https://archibus.vodacom.co.za/_Incapsula_Resource?SWJIYLWA=719d34d31c8e3a6e6fffd425f7e032f3%22ns=31%22cb=292274561 response code: 200
GET https://archibus.vodacom.co.za/_Incapsula_Resource?SWJIYLWA=719d34d31c8e3a6e6fffd425f7e032f3&ns=31&cb=292274561 response code: 200
GET https://archibus.vodacom.co.za/_Incapsula_Resource?SWKMTFSR=1&e=0.8762218735550797 response code: 200
GET https://archibus.vodacom.co.za/_Incapsula_Resource?SWKMTFSR=1&e=0.20939986879542816 response code: 200
GET https://archibus.vodacom.co.za/_Incapsula_Resource?SWJIYLWA=719d34d31c8e3a6e6fffd425f7e032f3%22ns=33%22cb=462486625 response code: 200
GET https://archibus.vodacom.co.za/_Incapsula_Resource?SWKMTFSR=1&e=0.657332483118807 response code: 200
GET https://archibus.vodacom.co.za/_Incapsula_Resource?SWJIYLWA=719d34d31c8e3a6e6fffd425f7e032f3%22ns=40%22cb=1925770764 response code: 200
GET https://archibus.vodacom.co.za/_Incapsula_Resource?SWJIYLWA=719d34d31c8e3a6e6fffd425f7e032f3%22ns=57%22cb=149715920 response code: 200
GET https://archibus.vodacom.co.za/_Incapsula_Resource?SWKMTFSR=1&e=0.9411161046872494 response code: 200
GET https://archibus.vodacom.co.za/_Incapsula_Resource?SWJIYLWA=719d34d31c8e3a6e6fffd425f7e032f3%22ns=62%22cb=759071798 response code: 200
GET https://archibus.vodacom.co.za/manager/ response code: 404
GET https://archibus.vodacom.co.za/_Incapsula_Resource?SWJIYLWA=719d34d31c8e3a6e6fffd425f7e032f3%22ns=63%22cb=261016948 response code: 200
GET https://archibus.vodacom.co.za/_Incapsula_Resource?SWKMTFSR=1&e=0.10408580974368586 response code: 200
GET https://archibus.vodacom.co.za/_Incapsula_Resource?SWKMTFSR=1&e=0.748959364503075 response code: 200
GET https://archibus.vodacom.co.za/host-manager/ response code: 404
GET https://archibus.vodacom.co.za/_Incapsula_Resource?CWUDNSAI=23%22xinfo=11-128333115-0%200NNN%20RT%281686510547447%202871%29%20q%280%20-1%20-1%200%29%20r%280%20-1%29%20B15%284%2c200%2c0%29%20U18%22incident_id=769000980359807166-61208577520232667%22edet=15%22cinfo=04000000%22rpinfo=0%22mth=GET response code: 404

150249 Misconfigured Header: Cache-Control (1)

150249 Misconfigured Header: Cache-Control

archibus.vodacom.co.za/archibus

Finding #	10541471	**Severity**	Information Gathered - Level 2
Unique #	ed023b99-db36-4e52-bd4a-8afab1803c22		
Group	Security Weaknesses		
CWE	CWE-525	**Detection Date**	11 Feb 2024 21:02 GMT+0200
OWASP	A5 Security Misconfiguration		
WASC	-		

Details

Threat

Cache-Control header present but directives may not configured to adequately safeguard sensitive information.

For Example:
Cache-Control directive set to public.

max-age value is greater than 86400.

Impact

If directive is set to public, the resource can be stored by any cache.

If max-age value is greater than 86400 for sensitive information may lead to information leakage.

Solution

Please check that resources with sensitive information are not configured with Cache-Control public directive.

Also please make sure that max-age directive value set properly to not cache sensitive information for longer period than needed.

References:
Mozilla Documentation Cache-Control

WAS Web Application Report

Results

Cache-Control: Header misconfigured. Cache-Control public directive found.
Cache-Control:max-age=86380, public on the link: GET https://archibus.vodacom.co.za/favicon.ico response code: 200

Cache-Control: Header misconfigured. Cache-Control public directive found.
Cache-Control:max-age=22, public on the link: GET https://archibus.vodacom.co.za/Leasure-the-deed-will-the-clipt-Angely-ands-Banq response code: 200

Cache-Control: Header misconfigured. Cache-Control public directive found.
Cache-Control:max-age=86381, public on the link: GET https://archibus.vodacom.co.za/tomcat.css response code: 200

Cache-Control: Header misconfigured. Cache-Control public directive found.
Cache-Control:max-age=5, public on the link: GET https://archibus.vodacom.co.za/Leasure-the-deed-will-the-clipt-Angely-ands-Banq?d=archibus.vodacom.co.za response code: 200

150262 Missing header: Feature-Policy (1)

150262 Missing header: Feature-Policy

archibus.vodacom.co.za/archibus

Finding #	10510595	**Severity**	Information Gathered - Level 2
Unique #	bf479622-6633-4d42-8a78-664c22333dd3		
Group	Security Weaknesses		
CWE	CWE-16, CWE-1032	**Detection Date**	11 Feb 2024 21:02 GMT+0200
OWASP	A5 Security Misconfiguration		
WASC	WASC-15 APPLICATION MISCONFIGURATION		

Details

Threat

The Feature-Policy response header is not present.

Impact

Feature Policy allows web developers to selectively enable, disable, and modify the behavior of certain APIs and web features such as "geolocation","camera", "usb", "fullscreen", "animations" etc in the browser.

These policies restrict what APIs the site can access or modify the browser's default behavior for certain features.

Solution

It is recommended to set the Feature-Policy header to selectively enable, disable, and modify the behavior of certain APIs and web features.

References:
- https://www.w3.org/TR/feature-policy/
- https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/Feature-Policy

Results

Feature-Policy: Header missing
Response headers on link: GET https://archibus.vodacom.co.za/favicon.ico response code: 200
cache-control: max-age=86380, public
content-length: 21630
content-security-policy-report-only: default-src 'self' 'unsafe-eval' 'unsafe-hashes' 'unsafe-inline' data: blob: ; form-action 'none' data: blob: ; report-uri /csp_report
content-type: image/x-icon
date: Sun, 11 Feb 2024 19:03:38 GMT
etag: W/"21630-1648737254000"
expires: Mon, 12 Feb 2024 19:03:18 GMT
last-modified: Thu, 31 Mar 2022 14:34:14 GMT
x-cdn: Imperva
x-iinfo: 60-17038774-0 0CNN RT(1707678198155 20620) q(0 -1 -1 -1) r(0 -1)
Set-Cookie: visid_incap_2776849=2mCPlvHbTaSKgOs2WBZQC/YZyWUAAAAAQUIPAAAAAAAWwMvjPe13zMYdphiXlTQy; HttpOnly; expires=Sun, 09-Feb-2025 22:21:11 GMT; domain=.vodacom.co.za; path=/
Set-Cookie: nlbi_2776849=ogi1WuqyhRkuEuYJZU49BAAAAABLcyLrdKjEmQdibbXYNFmh; domain=.vodacom.co.za; path=/

Set-Cookie: incap_ses_1687_2776849=9uxXXci+jlSe7PgfvG1pF/YZyWUAAAAAfr+BmEPjvWAiYHFjqA+aDQ==; domain=.vodacom.co.za; path=/

Header missing on the following link(s):
(Only first 50 such pages are listed)

GET https://archibus.vodacom.co.za/favicon.ico response code: 200
GET https://archibus.vodacom.co.za/FPRWin/index.aspx response code: 401
GET https://archibus.vodacom.co.za/Leasure-the-deed-will-the-clipt-Angely-ands-Banq response code: 200
GET https://archibus.vodacom.co.za/tomcat.css response code: 200
GET https://archibus.vodacom.co.za/docs/ response code: 404
GET https://archibus.vodacom.co.za/docs/config/ response code: 404
GET https://archibus.vodacom.co.za/examples/ response code: 404
GET https://archibus.vodacom.co.za/docs/security-howto.html response code: 404
GET https://archibus.vodacom.co.za/docs/manager-howto.html response code: 404
GET https://archibus.vodacom.co.za/docs/cluster-howto.html response code: 404
GET https://archibus.vodacom.co.za/manager/status response code: 404
GET https://archibus.vodacom.co.za/manager/html response code: 404
GET https://archibus.vodacom.co.za/host-manager/html response code: 404
GET https://archibus.vodacom.co.za/docs/setup.html response code: 404
GET https://archibus.vodacom.co.za/docs/appdev/ response code: 404
GET https://archibus.vodacom.co.za/docs/realm-howto.html response code: 404
GET https://archibus.vodacom.co.za/docs/jndi-datasource-examples-howto.html response code: 404
GET https://archibus.vodacom.co.za/docs/RELEASE-NOTES.txt response code: 404
GET https://archibus.vodacom.co.za/docs/api/index.html response code: 404
GET https://archibus.vodacom.co.za/docs/changelog.html response code: 404
GET https://archibus.vodacom.co.za/docs/deployer-howto.html response code: 404
GET https://archibus.vodacom.co.za/_Incapsula_Resource?SWJIYLWA=719d34d31c8e3a6e6fffd425f7e032f3&ns=19&cb=1246563959 response code: 200
GET https://archibus.vodacom.co.za/_Incapsula_Resource?SWJIYLWA=719d34d31c8e3a6e6fffd425f7e032f3&ns=5&cb=2085785877 response code: 200
GET https://archibus.vodacom.co.za/FPRWin/ response code: 401
GET https://archibus.vodacom.co.za/_Incapsula_Resource?SWJIYLWA=719d34d31c8e3a6e6fffd425f7e032f3%22ns=10%22cb=718590515 response code: 200
GET https://archibus.vodacom.co.za/Leasure-the-deed-will-the-clipt-Angely-ands-Banq?d=archibus.vodacom.co.za response code: 200
GET https://archibus.vodacom.co.za/_Incapsula_Resource?SWKMTFSR=1&e=0.3450785737536535 response code: 200
GET https://archibus.vodacom.co.za/_Incapsula_Resource?SWJIYLWA=719d34d31c8e3a6e6fffd425f7e032f3&ns=10&cb=718590515 response code: 200
GET https://archibus.vodacom.co.za/_Incapsula_Resource?SWJIYLWA=719d34d31c8e3a6e6fffd425f7e032f3&ns=30&cb=757409821 response code: 200
GET https://archibus.vodacom.co.za/_Incapsula_Resource?SWJIYLWA=719d34d31c8e3a6e6fffd425f7e032f3%22ns=23%22cb=682184485 response code: 200
GET https://archibus.vodacom.co.za/_Incapsula_Resource?SWKMTFSR=1&e=0.5272987180813904 response code: 200
GET https://archibus.vodacom.co.za/_Incapsula_Resource?SWJIYLWA=719d34d31c8e3a6e6fffd425f7e032f3&ns=23&cb=682184485 response code: 200
GET https://archibus.vodacom.co.za/_Incapsula_Resource?SWJIYLWA=719d34d31c8e3a6e6fffd425f7e032f3&ns=49&cb=1264811833 response code: 200
GET https://archibus.vodacom.co.za/_Incapsula_Resource?SWJIYLWA=719d34d31c8e3a6e6fffd425f7e032f3&ns=52&cb=1058230007 response code: 200
GET https://archibus.vodacom.co.za/_Incapsula_Resource?SWJIYLWA=719d34d31c8e3a6e6fffd425f7e032f3%22ns=31%22cb=292274561 response code: 200
GET https://archibus.vodacom.co.za/_Incapsula_Resource?SWJIYLWA=719d34d31c8e3a6e6fffd425f7e032f3&ns=31&cb=292274561 response code: 200
GET https://archibus.vodacom.co.za/_Incapsula_Resource?SWKMTFSR=1&e=0.8762218735550797 response code: 200
GET https://archibus.vodacom.co.za/_Incapsula_Resource?SWKMTFSR=1&e=0.20939986879542816 response code: 200
GET https://archibus.vodacom.co.za/_Incapsula_Resource?SWJIYLWA=719d34d31c8e3a6e6fffd425f7e032f3%22ns=33%22cb=462486625 response code: 200
GET https://archibus.vodacom.co.za/_Incapsula_Resource?SWKMTFSR=1&e=0.657332483118807 response code: 200
GET https://archibus.vodacom.co.za/_Incapsula_Resource?SWJIYLWA=719d34d31c8e3a6e6fffd425f7e032f3%22ns=40%22cb=1925770764 response code: 200
GET https://archibus.vodacom.co.za/_Incapsula_Resource?SWJIYLWA=719d34d31c8e3a6e6fffd425f7e032f3%22ns=57%22cb=149715920 response code: 200
GET https://archibus.vodacom.co.za/_Incapsula_Resource?SWKMTFSR=1&e=0.9411161046872494 response code: 200
GET https://archibus.vodacom.co.za/_Incapsula_Resource?SWJIYLWA=719d34d31c8e3a6e6fffd425f7e032f3%22ns=62%22cb=759071798 response code: 200
GET https://archibus.vodacom.co.za/manager/ response code: 404
GET https://archibus.vodacom.co.za/_Incapsula_Resource?SWJIYLWA=719d34d31c8e3a6e6fffd425f7e032f3%22ns=63%22cb=261016948 response code: 200
GET https://archibus.vodacom.co.za/_Incapsula_Resource?SWKMTFSR=1&e=0.10408580974368586 response code: 200
GET https://archibus.vodacom.co.za/_Incapsula_Resource?SWKMTFSR=1&e=0.748959364503075 response code: 200
GET https://archibus.vodacom.co.za/host-manager/ response code: 404
GET https://archibus.vodacom.co.za/_Incapsula_Resource?CWUDNSAI=23%22xinfo=11-128333115-0%200NNN%20RT%281686510547447%202871%29%20q%280%20-1%20-1%200%29%20r%280%20-1%29%20B15%284%2c200%2c0%29%20U18%22incident_id=76900098035980716 6-612085775202326667%22edet=15%22cinfo=04000000%22rpinfo=0%22mth=GET response code: 404

150101 Third-party Cookies Collected (1)

150101 Third-party Cookies Collected

archibus.vodacom.co.za/archibus

Finding #	14172490	**Severity**	Information Gathered - Level 1
Unique #	64dca8c7-6901-404f-9c72-8699d406d8eb		
Group	Security Weaknesses		
CWE	-	**Detection Date**	11 Feb 2024 21:02 GMT+0200
OWASP	-		
WASC	-		

Details

Threat

The cookies listed in the Results section were received from third-party web application(s) during the crawl phase.

Impact

Cookies may contain sensitive information about the user. Cookies sent via HTTP may be sniffed.

Solution
Review cookie values to ensure that sensitive information such as passwords are not present within them.

Results

Total cookies: 3
visid_incap_2653607=5WyHTAoQTwOQASGxHqHFwPYZyWUAAAAAQUIPAAAAAAAv++5Sd7WI0erJwGETz3BS; HttpOnly; expires=Sun, 09-Feb-2025 22:21:08 GMT; domain=.sso.vodacom.co.za; path=/ First set at URL: https://archibus.vodacom.co.za/archibus/
incap_ses_1687_2653607=pVjWcBFg02Oo7PgfvG1pF/YZyWUAAAAAI+PNsdwCbDKGdroEybsU0w==; domain=.sso.vodacom.co.za; path=/ First set at URL: https://archibus.vodacom.co.za/archibus/
nlbi_2653607_2147483392=ph9bJJxIAXaVCw2VoHFvpQAAAAAk8dnUexHo3DCUpnHVyO/T; domain=.sso.vodacom.co.za; path=/ First set at URL: https://archibus.vodacom.co.za/archibus/

150126 Links With High Resource Consumption (1)

150126 Links With High Resource Consumption — *archibus.vodacom.co.za/archibus*

Finding #	14172493	**Severity**	Information Gathered - Level 1
Unique #	fbfc503c-4a87-4b5d-9e3e-7eb0289c28ff		
Group	Security Weaknesses		
CWE	-	**Detection Date**	11 Feb 2024 21:02 GMT+0200
OWASP	-		
WASC	-		

Details

Threat
The list of links with lowest bytes/sec which are assumed to be resources with highest resource consumption. The links in the list have slower transfer times speeds to an average resource on the server. This may indicate that the links are more CPU or DB intensive than majority of links.

The latency of the network and file size have no effect on calculations.

Impact
The links with high resource consumption could be used to perform DOS on the server by just performing GET Flooding. Attackers could more easily take the server down if there are huge resource hogs on it, performing less request.

Solution
Find the root cause of resources slow download speed.

If the cause is a real CPU strain or complex DB queries performed, there may be a need for re-engineering of the web application or defense measures should be in place. Examples of defense against DOS that is targeted towards high resource consumption links are Load Balancers and Rate Limiters.

Results

0.000000 bytes/sec https://archibus.vodacom.co.za/_Incapsula_Resource?SWJIYLWA=719d34d31c8e3a6e6fffd425f7e032f3%22ns=10%22cb=718590515
0.000000 bytes/sec https://archibus.vodacom.co.za/_Incapsula_Resource?SWJIYLWA=719d34d31c8e3a6e6fffd425f7e032f3%22ns=23%22cb=682184485
0.000000 bytes/sec https://archibus.vodacom.co.za/_Incapsula_Resource?SWJIYLWA=719d34d31c8e3a6e6fffd425f7e032f3%22ns=33%22cb=462486625
0.000000 bytes/sec https://archibus.vodacom.co.za/_Incapsula_Resource?SWJIYLWA=719d34d31c8e3a6e6fffd425f7e032f3%22ns=40%22cb=1925770764
0.000000 bytes/sec https://archibus.vodacom.co.za/_Incapsula_Resource?SWJIYLWA=719d34d31c8e3a6e6fffd425f7e032f3%22ns=57%22cb=149715920
0.000000 bytes/sec https://archibus.vodacom.co.za/_Incapsula_Resource?SWJIYLWA=719d34d31c8e3a6e6fffd425f7e032f3%22ns=62%22cb=759071798
0.000000 bytes/sec https://archibus.vodacom.co.za/_Incapsula_Resource?SWJIYLWA=719d34d31c8e3a6e6fffd425f7e032f3%22ns=78%22cb=352187491
0.000000 bytes/sec https://archibus.vodacom.co.za/_Incapsula_Resource?SWJIYLWA=719d34d31c8e3a6e6fffd425f7e032f3%22ns=87%22cb=669575803
0.000000 bytes/sec https://archibus.vodacom.co.za/_Incapsula_Resource?SWJIYLWA=719d34d31c8e3a6e6fffd425f7e032f3%22ns=88%22cb=1925157912
0.000000 bytes/sec https://archibus.vodacom.co.za/_Incapsula_Resource?SWJIYLWA=719d34d31c8e3a6e6fffd425f7e032f3%22ns=98%22cb=1649221342

150135 HTTP Strict Transport Security (HSTS) header missing or misconfigured (1)

WAS Web Application Report

150135 HTTP Strict Transport Security (HSTS) header missing or misconfigured

archibus.vodacom.co.za/archibus

Finding #	10510596	**Severity**	Information Gathered - Level 1
Unique #	82250934-18dd-4e64-9ca2-9e7ea33c4a11		
Group	Security Weaknesses		
CWE	CWE-523	**Detection Date**	11 Feb 2024 21:02 GMT+0200
OWASP	A5 Security Misconfiguration		
WASC	-		

Details

Threat

HTTP Strict Transport Security (HSTS) header was found to be missing or misconfigured. The HSTS header instructs browsers that all subsequent connections to the website, for a configurable amount of time, should be performed over a secure (HTTPS) connection only. Additionally, it instructs browsers that users should not be permitted to bypass SSL/TLS certificate errors, in the event of an expired or otherwise untrusted certificate for example.

Impact

If HSTS header is not set, users are potentially vulnerable to man-in-the-middle (MITM) attacks, SSL stripping, and passive eavesdropper attacks.

Solution

For information about how to implement the HSTS header properly, refer to the OWASP HTTP Strict Transport Security Cheat Sheet.

Results

Strict Transport Security header missing for
https://archibus.vodacom.co.za/_Incapsula_Resource?CWUDNSAI=23&xinfo=9-67061412-0%200NNN%20RT%2816810668521 39%207%29%20q%280%20-1%20-1%20-1%29%20r%280%20-1%29%20B15%284%2c200%2c0%29%20U18&incident_id=766000980317811993-326349297580644489&edet=15&cinfo=04000000&rpinfo=0&mth=GET

150142 Virtual Host Discovered (1)

150142 Virtual Host Discovered

archibus.vodacom.co.za/archibus

Finding #	14172495	**Severity**	Information Gathered - Level 1
Unique #	d597b0ec-82e6-40f2-b0ad-5014be1f88e1		
Group	Security Weaknesses		
CWE	CWE-200	**Detection Date**	11 Feb 2024 21:02 GMT+0200
OWASP	A5 Security Misconfiguration		
WASC	-		

Details

Threat

Web server is responding differently when the HOST header is manipulated and various common virtual hosts are tested. This could indicate the presence of Virtual Host. Virtual hosting is a method for hosting multiple domain names (with separate handling of each name) on a single server (or pool of servers). This allows one server to share its resources, such as memory and processor cycles, without requiring all services provided to use the same host name. The extra virtual hosts discovered by the Web application scanner during HOST header manipulation are provided in the Results section.

Impact

The Web application should apply consistent security measures. If the Web application fails to apply security controls to other domains hosted on the same server, then it may be exposed to vulnerabilities like cross-site scripting, SQL injection, or authorization-based attacks.

Solution

Consult the virtual host configuration and check if this virtual host should be publicly accessible.

WAS Web Application Report

Results

Virtual host discovered:

Detected based on: HTTP Response code
Virtual Host: web.vodacom.co.za
URI: https://archibus.vodacom.co.za/

150204 Missing header: X-XSS-Protection (1)

150204 Missing header: X-XSS-Protection — *archibus.vodacom.co.za/archibus*

Finding #	10510604	**Severity**	Information Gathered - Level 1
Unique #	78520a52-b1e6-439d-afb6-178d1975323f		
Group	Security Weaknesses		
CWE	CWE-16, CWE-1032	**Detection Date**	11 Feb 2024 21:02 GMT+0200
OWASP	A5 Security Misconfiguration		
WASC	WASC-15 APPLICATION MISCONFIGURATION		

Details

Threat
The X-XSS-Protection response header is not present.

Impact
The X-XSS-Protection response header provides a layer of protection against reflected cross-site scripting (XSS) attacks by instructing browsers to abort rendering a page in which a reflected XSS attack has been detected. This is a best-effort second line of defense measure which helps prevent an attacker from using evasion techniques to avoid the neutralization mechanisms that the filters use by default. When configured appropriately, browser-level XSS filters can provide additional layers of defense against web application attacks.

Note that HTTP 4xx and 5xx responses can also be susceptible to attacks such as XSS. For better security the X-XSS-Protection header should be set on 4xx and 5xx responses as well.

Solution
It is recommend to set X-XSS-Protection header with value set to '1; mode=block' on all the relevant responses to activate browser's XSS filter.

NOTE: The X-XSS-Protection header is not supported by all browsers. Google Chrome and Safari are some of the browsers which support it, Firefox on the other hand does not support the header. X-XSS-Protection header does not guarantee a complete protection against XSS. For better protection against XSS attacks, the web application should use secure coding principles. Also, consider leveraging the Content-Security-Policy (CSP) header, which is supported by all browsers.

Using X-XSS-Protection could have unintended side effects, please understand the implications carefully before using it.

References:
- https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/X-XSS-Protection
- https://blog.innerht.ml/the-misunderstood-x-xss-protection/
- https://www.mbsd.jp/blog/20160407.html
- https://www.chromium.org/developers/design-documents/xss-auditor

Results

X-Xss-Protection: Header missing
Response headers on link: GET https://archibus.vodacom.co.za/FPRWin/index.aspx response code: 401
Connection: close
Content-Encoding: gzip
Content-Security-Policy-Report-Only: default-src 'self' 'unsafe-eval' 'unsafe-hashes' 'unsafe-inline' data: blob: ; form-action 'none' data: blob: ; report-uri /csp_report

Content-Type: text/html
Date: Sun, 11 Feb 2024 19:03:44 GMT
Instance: /ITG/pool_archibus_8080 10.134.16.81 8080
Server: Microsoft-IIS/10.0
Transfer-Encoding: chunked
WWW-Authenticate: Negotiate
X-CDN: Imperva
X-Frame-Options: SAMEORIGIN
X-Iinfo: 51-9164824-9164826 ENYy RT(1707678223948 174) q(0 0 0 -1) r(1 1) U16
X-Powered-By: ASP.NET
Set-Cookie: visid_incap_2776849=2mCPlvHbTaSKgOs2WBZQC/YZyWUAAAAAQUIPAAAAAAAWwMvjPe13zMYdphiXlTQy; HttpOnly; expires=Sun, 09-Feb-2025 22:21:11 GMT; domain=.vodacom.co.za; path=/
Set-Cookie: nlbi_2776849=ogi1WuqyhRkuEuYJZU49BAAAAABLcyLrdKjEmQdibbXYNFmh; domain=.vodacom.co.za; path=/
Set-Cookie: incap_ses_1687_2776849=9uxXXci+jlSe7PgfvG1pF/YZyWUAAAAAfr+BmEPjvWAiYHFjqA+aDQ==; domain=.vodacom.co.za; path=/
Set-Cookie: nlbi_2776849_2147483392=XMT0KRDY20D/IVChZU49BAAAAAA352epqdF/yOosCbwaXEXg; domain=.vodacom.co.za; path=/

Header missing on the following link(s):
(Only first 50 such pages are listed)

GET https://archibus.vodacom.co.za/FPRWin/index.aspx response code: 401
GET https://archibus.vodacom.co.za/docs/ response code: 404
GET https://archibus.vodacom.co.za/docs/config/ response code: 404
GET https://archibus.vodacom.co.za/examples/ response code: 404
GET https://archibus.vodacom.co.za/docs/security-howto.html response code: 404
GET https://archibus.vodacom.co.za/docs/manager-howto.html response code: 404
GET https://archibus.vodacom.co.za/docs/cluster-howto.html response code: 404
GET https://archibus.vodacom.co.za/manager/status response code: 404
GET https://archibus.vodacom.co.za/manager/html response code: 404
GET https://archibus.vodacom.co.za/host-manager/html response code: 404
GET https://archibus.vodacom.co.za/docs/setup.html response code: 404
GET https://archibus.vodacom.co.za/docs/appdev/ response code: 404
GET https://archibus.vodacom.co.za/docs/realm-howto.html response code: 404
GET https://archibus.vodacom.co.za/docs/jndi-datasource-examples-howto.html response code: 404
GET https://archibus.vodacom.co.za/docs/RELEASE-NOTES.txt response code: 404
GET https://archibus.vodacom.co.za/docs/api/index.html response code: 404
GET https://archibus.vodacom.co.za/docs/changelog.html response code: 404
GET https://archibus.vodacom.co.za/docs/deployer-howto.html response code: 404
GET https://archibus.vodacom.co.za/FPRWin/ response code: 401
GET https://archibus.vodacom.co.za/_Incapsula_Resource?SWKMTFSR=1&e=0.3450785737536535 response code: 200
GET https://archibus.vodacom.co.za/_Incapsula_Resource?SWKMTFSR=1&e=0.5272987180813904 response code: 200
GET https://archibus.vodacom.co.za/_Incapsula_Resource?SWKMTFSR=1&e=0.8762218735550797 response code: 200
GET https://archibus.vodacom.co.za/_Incapsula_Resource?SWKMTFSR=1&e=0.20939986879542816 response code: 200
GET https://archibus.vodacom.co.za/_Incapsula_Resource?SWKMTFSR=1&e=0.657332483118807 response code: 200
GET https://archibus.vodacom.co.za/_Incapsula_Resource?SWKMTFSR=1&e=0.9411161046872494 response code: 200
GET https://archibus.vodacom.co.za/manager/ response code: 404
GET https://archibus.vodacom.co.za/_Incapsula_Resource?SWKMTFSR=1&e=0.10408580974368586 response code: 200
GET https://archibus.vodacom.co.za/_Incapsula_Resource?SWKMTFSR=1&e=0.748959364503075 response code: 200
GET https://archibus.vodacom.co.za/host-manager/ response code: 404
GET https://archibus.vodacom.co.za/docs/api/ response code: 404
GET https://archibus.vodacom.co.za/_Incapsula_Resource?CWUDNSAI=23%22xinfo=11-128333115-0%200NNN%20RT%281686510547447%202871%29%20q%280%20-1%20-1%200%29%20r%280%20-1%29%20B15%284%2c200%2c0%29%20U18%22incident_id=76900980359807166-612085775202326667%22edet=15%22cinfo=04000000%22rpinfo=0%22mth=GET response code: 404
GET https://archibus.vodacom.co.za/_Incapsula_Resource?CWUDNSAI=23%22xinfo=11-74601801-0%200NNN%20RT%281694372516063%202785%29%20q%280%20-1%20-1%200%29%20r%280%20-1%29%20B15%284%2c200%2c0%29%20U18%22incident_id=76400041017990764-353379304890698315%22edet=15%22cinfo=04000000%22rpinfo=0%22mth=GET response code: 404
GET https://archibus.vodacom.co.za/_Incapsula_Resource?CWUDNSAI=23%22xinfo=12-140568936-0%200NNN%20RT%281699815739671%202292%29%20q%280%20-1%20-1%201%29%20r%280%20-1%29%20B15%284%2c200%2c0%29%20U18%22incident_id=76601190516980779-773471142739320268%22edet=15%22cinfo=04000000%22rpinfo=0%22mth=GET response code: 404
GET https://archibus.vodacom.co.za/_Incapsula_Resource?CWUDNSAI=23%22xinfo=13-51475396-0%200NNN%20RT%281696791744809%202625%29%20q%280%20-1%20-1%202%29%20r%280%20-1%29%20B15%284%2c200%2c0%29%20U18%22incident_id=76400046012960 3047-261986575540030349%22edet=15%22cinfo=04000000%22rpinfo=0%22mth=GET response code: 404
GET https://archibus.vodacom.co.za/_Incapsula_Resource?CWUDNSAI=23%22xinfo=4-9346511-0%200NNN%20RT%281694372516064%2015875%29%20q%280%20-1%20-1%200%29%20r%280%20-1%29%20B15%284%2c200%2c0%29%20U18%22incident_id=76400041017990764-45602206157376068%22edet=15%22cinfo=04000000%22rpinfo=0%22mth=GET response code: 404
GET https://archibus.vodacom.co.za/_Incapsula_Resource?CWUDNSAI=23%22xinfo=14-56552041-0%200NNN%20RT%281684091004822%202271%29%20q%280%20-1%20-1%200%29%20r%280%20-1%29%20B15%284%2c200%2c0%29%20U18%22incident_id=76800033012684013 8-290605261188499534%22edet=15%22cinfo=04000000%22rpinfo=0%22mth=GET response code: 404
GET https://archibus.vodacom.co.za/_Incapsula_Resource?CWUDNSAI=23%22xinfo=7-120841302-0%200NNN%20RT%281688929454119%2016073%29%20q%280%20-1%20-1%200%29%20r%280%20-1%29%20B15%284%2c200%2c0%29%20U18%22incident_id=44900158057159480 0-631738012224530311%22edet=15%22cinfo=04000000%22rpinfo=0%22mth=GET response code: 404
GET https://archibus.vodacom.co.za/_Incapsula_Resource?CWUDNSAI=23%22xinfo=13-51475397-0%200NNN%20RT%281696791744809%2015891%29%20q%280%20-1%20-1%200%29%20r%280%20-1%29%20B15%284%2c200%2c0%29%20U18%22incident_id=76400046012960 3047-26200120419864052 5%22edet=15%22cinfo=04000000%22rpinfo=0%22mth=GET response code: 404
GET https://archibus.vodacom.co.za/_Incapsula_Resource?CWUDNSAI=23%22xinfo=12-143394600-0%200NNN%20RT%281691953410996%20780%29%20q%280%20-1%20-1%200%29%20r%280%20-1%29%20B15%284%2c200%2c0%29%20U18%22incident_id=12800073032438 6403-6886943938544973 56%22edet=15%22cinfo=04000000%22rpinfo=0%22mth=GET response code: 404
GET https://archibus.vodacom.co.za/_Incapsula_Resource?CWUDNSAI=23%22xinfo=13-133113832-0%200NNN%20RT%281699815739671%2015870%29%20q%280%20-1%20-1%200%29%20r%280%20-1%29%20B15%284%2c200%2c0%29%20U18%22incident_id=76601190516980779-728228691682663885%22edet=15%22cinfo=04000000%22rpinfo=0%22mth=GET response code: 404
GET https://archibus.vodacom.co.za/_Incapsula_Resource?CWUDNSAI=23%22xinfo=8-71777546-0%200NNN%20RT%281691953415895%209146%29%20q%280%20-1%20-1%202%29%20r%280%20-1%29%20B15%284%2c200%2c0%29%20U18%22incident_id=12800073032438 6403-355359155923456584%22edet=15%22cinfo=04000000%22rpinfo=0%22mth=GET response code: 404
GET https://archibus.vodacom.co.za/_Incapsula_Resource?CWUDNSAI=23%22xinfo=6-50761907-0%200NNN%20RT%281691953429171%2013568%29%20q%280%20-1%20-1%200%29%20r%280%20-1%29%20B15%284%2c200%2c0%29%20U18%22incident_id=12800073032438 6403-257296789038699078%22edet=15%22cinfo=04000000%22rpinfo=0%22mth=GET response code: 404

GET https://archibus.vodacom.co.za/_Incapsula_Resource?CWUDNSAI=23%22xinfo=13-50005422-0%200NNN%20RT%281684091004823%2015780%29%20q%280%20-1%20-1%201%29%20r%280%20-1%29%20B15%284%2c200%2c0%29%20U18%22incident_id=768000330126840138-244105402621364301%22edet=15%22cinfo=04000000%22rpinfo=0%22mth=GET response code: 404
GET https://archibus.vodacom.co.za/_Incapsula_Resource?CWUDNSAI=23%22xinfo=5-218372829-0%200NNN%20RT%281688929454117%202786%29%20q%280%20-1%20-1%201%29%20r%280%20-1%29%20B15%284%2c200%2c0%29%20U18%22incident_id=449001580571594800-111895544297063411 7%22edet=15%22cinfo=04000000%22rpinfo=0%22mth=GET response code: 404
GET https://archibus.vodacom.co.za/_Incapsula_Resource?CWUDNSAI=23%22xinfo=10-112012598-0%200NNN%20RT%281691953444703%2013039%29%20q%280%20-1%20-1%204%29%20r%280%20-1%29%20B15%284%2c200%2c0%29%20U18%22incident_id=128000730324386403-546957586868474442%22edet=15%22cinfo=04000000%22rpinfo=0%22mth=GET response code: 404
GET https://archibus.vodacom.co.za/_Incapsula_Resource?CWUDNSAI=23%22xinfo=10-107502277-0%200NNN%20RT%281686510550324%2012994%29%20q%280%20-1%20-1%200%29%20r%280%20-1%29%20B15%284%2c200%2c0%29%20U18%22incident_id=769000980359807166-515218109305526410%22edet=15%22cinfo=04000000%22rpinfo=0%22mth=GET response code: 404
GET https://archibus.vodacom.co.za/_Incapsula_Resource?CWUDNSAI=23&xinfo=13-50005422-0%200NNN%20RT%281684091004823%2015780%29%20q%280%20-1%20-1%201%29%20r%280%20-1%29%20B15%284%2C200%2C0%29%20U18&incident_id=768000330126840138-244105402621364301&edet=15&cinfo=04000000&rpinfo=0&mth=GET response code: 200
GET https://archibus.vodacom.co.za/_Incapsula_Resource?CWUDNSAI=23&xinfo=13-51475396-0%200NNN%20RT%281696791744809%202625%29%20q%280%20-1%20-1%202%29%20r%280%20-1%29%20B15%284%2C200%2C0%29%20U18&incident_id=764000460129603047-261986575540030349&edet=15&cinfo=04000000&rpinfo=0&mth=GET response code: 200
GET https://archibus.vodacom.co.za/_Incapsula_Resource?CWUDNSAI=23&xinfo=14-178098704-0%200NNN%20RT%281681066855737%202281%29%20q%280%20-1%20-1%208%29%20r%280%20-1%29%20B15%284%2C200%2C0%29%20U18&incident_id=766000980317811993-862742334339422350&edet=15&cinfo=04000000&rpinfo=0&mth=GET response code: 200
GET https://archibus.vodacom.co.za/_Incapsula_Resource?CWUDNSAI=23&xinfo=13-51475397-0%200NNN%20RT%281696791744809%2015891%29%20q%280%20-1%20-1%200%29%20r%280%20-1%29%20B15%284%2C200%2C0%29%20U18&incident_id=764000460129603047-262001204198640525&edet=15&cinfo=04000000&rpinfo=0&mth=GET response code: 200

150245 Missing header: X-Frame-Options (1)

150245 Missing header: X-Frame-Options

archibus.vodacom.co.za/archibus

Finding #	10510587	**Severity**	Information Gathered - Level 1
Unique #	a3dc1997-5331-4e7a-b5bc-ea99ecd61e09		
Group	Security Weaknesses		
CWE	CWE-693	**Detection Date**	11 Feb 2024 21:02 GMT+0200
OWASP	A5 Security Misconfiguration		
WASC	WASC-15 APPLICATION MISCONFIGURATION		

Details

Threat

The X-Frame-Options header is not set in the HTTP response, meaning the page can potentially be loaded into an attacker-controlled frame. This could lead to clickjacking, where an attacker adds an invisible layer on top of the legitimate page to trick users into clicking on a malicious link or taking a harmful action.

Impact

Without an X-Frame-Options response header, clickjacking may be possible. However, if the application properly uses the Content-Security-Policy "frame-ancestors" directive, then modern web browsers would stop the page from being framed and prevent clickjacking.

Solution

The X-Frame-Options allows three values: DENY, SAMEORIGIN and ALLOW-FROM. It is recommended to use DENY, which prevents all domains from framing the page or SAMEORIGIN, which allows framing only by the same site. DENY and SAMEORGIN are supported by all browsers. Using ALLOW-FROM is not recommended because not all browsers support it.

Note: To avoid a common X-Frame-Options implementation mistake, see https://blog.qualys.com/securitylabs/2015/10/20/clickjacking-a-common-implementation-mistake-that-can-put-your-websites-in-danger.

Results

X-Frame-Options header is missing or not set to DENY or SAMEORIGIN for the following pages:
(Only first 10 such pages are reported)

GET https://archibus.vodacom.co.za/_Incapsula_Resource?CWUDNSAI=23&xinfo=13-50005422-0%200NNN%20RT%281684091004823%2015780%29%20q%280%20-1%20-1%201%29%20r%280%20-1%29%20B15%284%2C200%2C0%29%20U18&incident_id=768000330126840138-244105402621364301&edet=15&cinfo=04000000&rpinfo=0&mth=GET
Response code: 200
Response headers:
Cache-Control: no-cache, no-store
Content-Encoding: gzip
Content-Length: 3753
Content-Security-Policy-Report-Only: default-src 'self' 'unsafe-eval' 'unsafe-hashes' 'unsafe-inline' data: blob: ; form-action 'none' data: blob: ; report-uri /csp_report
Content-Type: text/html
X-Robots-Tag: noindex
Set-Cookie: visid_incap_2776849=2mCPlvHbTaSKgOs2WBZQC/YZyWUAAAAAQUIPAAAAAAAWwMvjPe13zMYdphiXlTQy; HttpOnly; expires=Sun, 09-Feb-2025 22:21:11 GMT; domain=.vodacom.co.za; path=/

Set-Cookie: nlbi_2776849=ogi1WuqyhRkuEuYJZU49BAAAAABLcyLrdKjEmQdibbXYNFmh; domain=.vodacom.co.za; path=/
Set-Cookie: incap_ses_1687_2776849=9uxXXci+jlSe7PgfvG1pF/YZyWUAAAAAfr+BmEPjvWAiYHFjqA+aDQ==; domain=.vodacom.co.za; path=/
Set-Cookie: nlbi_2776849_2147483392=v7a1dnMbPCfHqgN1ZU49BAAAAAAMGm8CgmVX0q6jtFAjZmEi; domain=.vodacom.co.za; path=/

GET https://archibus.vodacom.co.za/_Incapsula_Resource?CWUDNSAI=23&xinfo=13-51475396-0%200NNN%20RT%281696791744809%202625%29%20q%280%20-1%20-1%202%29%20r%280%20-1%29%20B15%284%2C200%2C0%29%20U18&incident_id=764000460129603047-261986575540030349&edet=15&cinfo=04000000&rpinfo=0&mth=GET
Response code: 200
Response headers:
Cache-Control: no-cache, no-store
Content-Encoding: gzip
Content-Length: 3757
Content-Security-Policy-Report-Only: default-src 'self' 'unsafe-eval' 'unsafe-hashes' 'unsafe-inline' data: blob: ; form-action 'none' data: blob: ; report-uri /csp_report
Content-Type: text/html
X-Robots-Tag: noindex
Set-Cookie: visid_incap_2776849=2mCPlvHbTaSKgOs2WBZQC/YZyWUAAAAAQUIPAAAAAAAWwMvjPe13zMYdphiXlTQy; HttpOnly; expires=Sun, 09-Feb-2025 22:21:11 GMT; domain=.vodacom.co.za; path=/
Set-Cookie: nlbi_2776849=ogi1WuqyhRkuEuYJZU49BAAAAABLcyLrdKjEmQdibbXYNFmh; domain=.vodacom.co.za; path=/
Set-Cookie: incap_ses_1687_2776849=9uxXXci+jlSe7PgfvG1pF/YZyWUAAAAAfr+BmEPjvWAiYHFjqA+aDQ==; domain=.vodacom.co.za; path=/
Set-Cookie: nlbi_2776849_2147483392=v7a1dnMbPCfHqgN1ZU49BAAAAAAMGm8CgmVX0q6jtFAjZmEi; domain=.vodacom.co.za; path=/

GET https://archibus.vodacom.co.za/_Incapsula_Resource?CWUDNSAI=23&xinfo=13-51475397-0%200NNN%20RT%281696791744809%2015891%29%20q%280%20-1%20-1%200%29%20r%280%20-1%29%20B15%284%2C200%2C0%29%20U18&incident_id=764000460129603047-262001204198640525&edet=15&cinfo=04000000&rpinfo=0&mth=GET
Response code: 200
Response headers:
Cache-Control: no-cache, no-store
Content-Encoding: gzip
Content-Length: 3756
Content-Security-Policy-Report-Only: default-src 'self' 'unsafe-eval' 'unsafe-hashes' 'unsafe-inline' data: blob: ; form-action 'none' data: blob: ; report-uri /csp_report
Content-Type: text/html
X-Robots-Tag: noindex
Set-Cookie: visid_incap_2776849=2mCPlvHbTaSKgOs2WBZQC/YZyWUAAAAAQUIPAAAAAAAWwMvjPe13zMYdphiXlTQy; HttpOnly; expires=Sun, 09-Feb-2025 22:21:11 GMT; domain=.vodacom.co.za; path=/
Set-Cookie: nlbi_2776849=ogi1WuqyhRkuEuYJZU49BAAAAABLcyLrdKjEmQdibbXYNFmh; domain=.vodacom.co.za; path=/
Set-Cookie: incap_ses_1687_2776849=9uxXXci+jlSe7PgfvG1pF/YZyWUAAAAAfr+BmEPjvWAiYHFjqA+aDQ==; domain=.vodacom.co.za; path=/
Set-Cookie: nlbi_2776849_2147483392=v7a1dnMbPCfHqgN1ZU49BAAAAAAMGm8CgmVX0q6jtFAjZmEi; domain=.vodacom.co.za; path=/

GET https://archibus.vodacom.co.za/_Incapsula_Resource?CWUDNSAI=23&xinfo=14-178098704-0%200NNN%20RT%281681066855737%202281%29%20q%280%20-1%20-1%208%29%20r%280%20-1%29%20B15%284%2C200%2C0%29%20U18&incident_id=766000980317811993-862742334339422350&edet=15&cinfo=04000000&rpinfo=0&mth=GET
Response code: 200
Response headers:
Cache-Control: no-cache, no-store
Content-Encoding: gzip
Content-Length: 3758
Content-Security-Policy-Report-Only: default-src 'self' 'unsafe-eval' 'unsafe-hashes' 'unsafe-inline' data: blob: ; form-action 'none' data: blob: ; report-uri /csp_report
Content-Type: text/html
X-Robots-Tag: noindex
Set-Cookie: visid_incap_2776849=2mCPlvHbTaSKgOs2WBZQC/YZyWUAAAAAQUIPAAAAAAAWwMvjPe13zMYdphiXlTQy; HttpOnly; expires=Sun, 09-Feb-2025 22:21:11 GMT; domain=.vodacom.co.za; path=/
Set-Cookie: nlbi_2776849=ogi1WuqyhRkuEuYJZU49BAAAAABLcyLrdKjEmQdibbXYNFmh; domain=.vodacom.co.za; path=/
Set-Cookie: incap_ses_1687_2776849=9uxXXci+jlSe7PgfvG1pF/YZyWUAAAAAfr+BmEPjvWAiYHFjqA+aDQ==; domain=.vodacom.co.za; path=/
Set-Cookie: nlbi_2776849_2147483392=v7a1dnMbPCfHqgN1ZU49BAAAAAAMGm8CgmVX0q6jtFAjZmEi; domain=.vodacom.co.za; path=/

GET https://archibus.vodacom.co.za/_Incapsula_Resource?CWUDNSAI=23&xinfo=14-178098704-0%200NNN%20RT%281681066855737%202281%29%20q%280%20-1%20-1%208%29%20r%280%20-1%29%20B15%284%2c200%2c0%29%20U18&incident_id=766000980317811993-862742334339422350&edet=15&cinfo=04000000&rpinfo=0&mth=GET
Response code: 200
Response headers:
Cache-Control: no-cache, no-store
Content-Encoding: gzip
Content-Length: 3758
Content-Security-Policy-Report-Only: default-src 'self' 'unsafe-eval' 'unsafe-hashes' 'unsafe-inline' data: blob: ; form-action 'none' data: blob: ; report-uri /csp_report
Content-Type: text/html
X-Robots-Tag: noindex
Set-Cookie: visid_incap_2776849=2mCPlvHbTaSKgOs2WBZQC/YZyWUAAAAAQUIPAAAAAAAWwMvjPe13zMYdphiXlTQy; HttpOnly; expires=Sun, 09-Feb-2025 22:21:11 GMT; domain=.vodacom.co.za; path=/
Set-Cookie: nlbi_2776849=ogi1WuqyhRkuEuYJZU49BAAAAABLcyLrdKjEmQdibbXYNFmh; domain=.vodacom.co.za; path=/
Set-Cookie: incap_ses_1687_2776849=9uxXXci+jlSe7PgfvG1pF/YZyWUAAAAAfr+BmEPjvWAiYHFjqA+aDQ==; domain=.vodacom.co.za; path=/
Set-Cookie: nlbi_2776849_2147483392=v7a1dnMbPCfHqgN1ZU49BAAAAAAMGm8CgmVX0q6jtFAjZmEi; domain=.vodacom.co.za; path=/

GET https://archibus.vodacom.co.za/_Incapsula_Resource?CWUDNSAI=23&xinfo=14-178100241-0%200NNN%20RT%281681066864525%202%29%20q%280%20-1%20-1%200%29%20r%280%20-1%29%20B15%284%2c200%2c0%29%20U18&incident_id=766000980317811993-862747269256845454&edet=15&cinfo=04000000&rpinfo=0&mth=GET
Response code: 200
Response headers:
Cache-Control: no-cache, no-store
Content-Encoding: gzip
Content-Length: 3759
Content-Security-Policy-Report-Only: default-src 'self' 'unsafe-eval' 'unsafe-hashes' 'unsafe-inline' data: blob: ; form-action 'none' data: blob: ; report-uri /csp_report
Content-Type: text/html
X-Robots-Tag: noindex
Set-Cookie: visid_incap_2776849=2mCPlvHbTaSKgOs2WBZQC/YZyWUAAAAAQUIPAAAAAAAWwMvjPe13zMYdphiXlTQy; HttpOnly; expires=Sun, 09-Feb-2025 22:21:11 GMT; domain=.vodacom.co.za; path=/
Set-Cookie: nlbi_2776849=ogi1WuqyhRkuEuYJZU49BAAAAABLcyLrdKjEmQdibbXYNFmh; domain=.vodacom.co.za; path=/
Set-Cookie: incap_ses_1687_2776849=9uxXXci+jlSe7PgfvG1pF/YZyWUAAAAAfr+BmEPjvWAiYHFjqA+aDQ==; domain=.vodacom.co.za; path=/
Set-Cookie: nlbi_2776849_2147483392=v7a1dnMbPCfHqgN1ZU49BAAAAAAMGm8CgmVX0q6jtFAjZmEi; domain=.vodacom.co.za; path=/

GET https://archibus.vodacom.co.za/_Incapsula_Resource?CWUDNSAI=23&xinfo=14-56552041-0%200NNN%20RT%281684091004822%202271%29%20q%280%20-1%20-1%200%29%20r

%280%20-1%29%20B15%284%2C200%2C0%29%20U18&incident_id=768000330126840138-290605261188499534&edet=15&cinfo=04000000&rpinfo=0&mth=GET
Response code: 200
Response headers:
Cache-Control: no-cache, no-store
Content-Encoding: gzip
Content-Length: 3754
Content-Security-Policy-Report-Only: default-src 'self' 'unsafe-eval' 'unsafe-hashes' 'unsafe-inline' data: blob: ; form-action 'none' data: blob: ; report-uri /csp_report
Content-Type: text/html
X-Robots-Tag: noindex
Set-Cookie: visid_incap_2776849=2mCPlvHbTaSKgOs2WBZQC/YZyWUAAAAAQUIPAAAAAAAWwMvjPe13zMYdphiXlTQy; HttpOnly; expires=Sun, 09-Feb-2025 22:21:11 GMT; domain=.vodacom.co.za; path=/
Set-Cookie: nlbi_2776849=ogi1WuqyhRkuEuYJZU49BAAAAABLcyLrdKjEmQdibbXYNFmh; domain=.vodacom.co.za; path=/
Set-Cookie: incap_ses_1687_2776849=9uxXXci+jlSe7PgfvG1pF/YZyWUAAAAAfr+BmEPjvWAiYHFjqA+aDQ==; domain=.vodacom.co.za; path=/
Set-Cookie: nlbi_2776849_2147483392=v7a1dnMbPCfHqgN1ZU49BAAAAAAMGm8CgmVX0q6jtFAjZmEi; domain=.vodacom.co.za; path=/

GET https://archibus.vodacom.co.za/_Incapsula_Resource?CWUDNSAI=23&xinfo=14-99576411-0%200NNN%20RT%281694372512606%209%29%20q%280%20-1%20-1%20-1%29%20r%280%20-1%29%20B15%284%2c200%2c0%29%20U18&incident_id=764000410179907764-464681797523606094&edet=15&cinfo=04000000&rpinfo=0&mth=GET
Response code: 200
Response headers:
Cache-Control: no-cache, no-store
Content-Encoding: gzip
Content-Length: 3757
Content-Security-Policy-Report-Only: default-src 'self' 'unsafe-eval' 'unsafe-hashes' 'unsafe-inline' data: blob: ; form-action 'none' data: blob: ; report-uri /csp_report
Content-Type: text/html
X-Robots-Tag: noindex
Set-Cookie: visid_incap_2776849=2mCPlvHbTaSKgOs2WBZQC/YZyWUAAAAAQUIPAAAAAAAWwMvjPe13zMYdphiXlTQy; HttpOnly; expires=Sun, 09-Feb-2025 22:21:11 GMT; domain=.vodacom.co.za; path=/
Set-Cookie: nlbi_2776849=ogi1WuqyhRkuEuYJZU49BAAAAABLcyLrdKjEmQdibbXYNFmh; domain=.vodacom.co.za; path=/
Set-Cookie: incap_ses_1687_2776849=9uxXXci+jlSe7PgfvG1pF/YZyWUAAAAAfr+BmEPjvWAiYHFjqA+aDQ==; domain=.vodacom.co.za; path=/
Set-Cookie: nlbi_2776849_2147483392=v7a1dnMbPCfHqgN1ZU49BAAAAAAMGm8CgmVX0q6jtFAjZmEi; domain=.vodacom.co.za; path=/

GET https://archibus.vodacom.co.za/_Incapsula_Resource?CWUDNSAI=23&xinfo=14-99580654-0%200NNN%20RT%281694372525149%204%29%20q%280%20-1%20-1%200%29%20r%280%20-1%29%20B15%284%2c200%2c0%29%20U18&incident_id=764000410179907764-464701605912775246&edet=15&cinfo=04000000&rpinfo=0&mth=GET
Response code: 200
Response headers:
Cache-Control: no-cache, no-store
Content-Encoding: gzip
Content-Length: 3755
Content-Security-Policy-Report-Only: default-src 'self' 'unsafe-eval' 'unsafe-hashes' 'unsafe-inline' data: blob: ; form-action 'none' data: blob: ; report-uri /csp_report
Content-Type: text/html
X-Robots-Tag: noindex
Set-Cookie: visid_incap_2776849=2mCPlvHbTaSKgOs2WBZQC/YZyWUAAAAAQUIPAAAAAAAWwMvjPe13zMYdphiXlTQy; HttpOnly; expires=Sun, 09-Feb-2025 22:21:11 GMT; domain=.vodacom.co.za; path=/
Set-Cookie: nlbi_2776849=ogi1WuqyhRkuEuYJZU49BAAAAABLcyLrdKjEmQdibbXYNFmh; domain=.vodacom.co.za; path=/
Set-Cookie: incap_ses_1687_2776849=9uxXXci+jlSe7PgfvG1pF/YZyWUAAAAAfr+BmEPjvWAiYHFjqA+aDQ==; domain=.vodacom.co.za; path=/
Set-Cookie: nlbi_2776849_2147483392=v7a1dnMbPCfHqgN1ZU49BAAAAAAMGm8CgmVX0q6jtFAjZmEi; domain=.vodacom.co.za; path=/

GET https://archibus.vodacom.co.za/_Incapsula_Resource?CWUDNSAI=23&xinfo=4-185001335-0%200NNN%20RT%281688929350663%207%29%20q%280%20-1%20-1%20-1%29%20r%280%20-1%29%20B15%284%2c200%2c0%29%20U18&incident_id=449001580571594800-949909193807177604&edet=15&cinfo=04000000&rpinfo=0&mth=GET
Response code: 200
Response headers:
Cache-Control: no-cache, no-store
Content-Encoding: gzip
Content-Length: 3758
Content-Security-Policy-Report-Only: default-src 'self' 'unsafe-eval' 'unsafe-hashes' 'unsafe-inline' data: blob: ; form-action 'none' data: blob: ; report-uri /csp_report
Content-Type: text/html
X-Robots-Tag: noindex
Set-Cookie: visid_incap_2776849=2mCPlvHbTaSKgOs2WBZQC/YZyWUAAAAAQUIPAAAAAAAWwMvjPe13zMYdphiXlTQy; HttpOnly; expires=Sun, 09-Feb-2025 22:21:11 GMT; domain=.vodacom.co.za; path=/
Set-Cookie: nlbi_2776849=ogi1WuqyhRkuEuYJZU49BAAAAABLcyLrdKjEmQdibbXYNFmh; domain=.vodacom.co.za; path=/
Set-Cookie: incap_ses_1687_2776849=9uxXXci+jlSe7PgfvG1pF/YZyWUAAAAAfr+BmEPjvWAiYHFjqA+aDQ==; domain=.vodacom.co.za; path=/
Set-Cookie: nlbi_2776849_2147483392=v7a1dnMbPCfHqgN1ZU49BAAAAAAMGm8CgmVX0q6jtFAjZmEi; domain=.vodacom.co.za; path=/

150277 Cookie without SameSite attribute (1)

150277 Cookie without SameSite attribute *archibus.vodacom.co.za/archibus*

Finding #	10510588	**Severity**	Information Gathered - Level 1
Unique #	4fa003b5-ada8-41bb-ad9e-f1d222b61c5f		
Group	Security Weaknesses		
CWE	CWE-16, CWE-1032	**Detection Date**	11 Feb 2024 21:02 GMT+0200
OWASP	A5 Security Misconfiguration		
WASC	-		

Details

Threat
The cookies listed in the Results section are missing the SameSite attribute.

Impact
The SameSite cookie attribute is an effective countermeasure against cross-site request forgery (CSRF) attacks. Note that a missing SameSite attribute does not mean the web application is automatically vulnerable to CSRF. The scanner will report QID 150071 if a CSRF vulnerability is detected.

Solution
Consider adding the SameSite attribute to the cookie(s) listed.

More information:
DZone article
OWASP CSRF Prevention Cheat Sheet

Results

Total cookies: 7
incap_ses_1687_2653607=pVjWcBFg02Oo7PgfvG1pF/YZyWUAAAAAI+PNsdwCbDKGdroEybsU0w==; path=/; domain=.sso.vodacom.co.za | First set at URL: https://archibus.vodacom.co.za/archibus/
incap_ses_1687_2776849=9uxXXci+jlSe7PgfvG1pF/YZyWUAAAAAfr+BmEPjvWAiYHFjqA+aDQ==; path=/; domain=.vodacom.co.za | First set at URL: https://archibus.vodacom.co.za/archibus/
nlbi_2653607_2147483392=ph9bJJxIAXaVCw2VoHFvpQAAAAAk8dnUexHo3DCUpnHVyO/T; path=/; domain=.sso.vodacom.co.za | First set at URL: https://archibus.vodacom.co.za/archibus/
nlbi_2776849=ogi1WuqyhRkuEuYJZU49BAAAAABLcyLrdKjEmQdibbXYNFmh; path=/; domain=.vodacom.co.za | First set at URL: https://archibus.vodacom.co.za/archibus/
nlbi_2776849_2147483392=XMT0KRDY20D/IVChZU49BAAAAAA352epqdF/yOosCbwaXEXg; path=/; domain=.vodacom.co.za | First set at URL: https://archibus.vodacom.co.za/FPRWin/index.aspx
visid_incap_2653607=5WyHTAoQTwOQASGxHqHFwPYZyWUAAAAAQUIPAAAAAAAv++5Sd7WI0erJwGETz3BS; expires=Sun Feb 9 22:21:08 2025; path=/; domain=.sso.vodacom.co.za; max-age=31459898; httponly | First set at URL: https://archibus.vodacom.co.za/archibus/
visid_incap_2776849=2mCPlvHbTaSKgOs2WBZQC/YZyWUAAAAAQUIPAAAAAAAWwMvjPe13zMYdphiXlTQy; expires=Sun Feb 9 22:21:11 2025; path=/; domain=.vodacom.co.za; max-age=31459901; httponly | First set at URL: https://archibus.vodacom.co.za/archibus/

archibus.vodacom.co.za:443/fpr/index.asp (48)

Vulnerability (7)

Path Disclosure (1)

150004 Path-Based Vulnerability (1)

150004 Path-Based Vulnerability — *archibus.vodacom.co.za:443/fpr/index.asp* **New**

URL: https://archibus.vodacom.co.za/docs/config/download/

Finding #	23855530	**Severity**	Confirmed Vulnerability - Level 2
Unique #	b253f232-5112-4690-97a4-d40b2aee8ad7		
Group	Path Disclosure	**First Time Detected**	11 Feb 2024 21:02 GMT+0200
CWE	CWE-22	**Last Time Detected**	11 Feb 2024 21:02 GMT+0200
OWASP	A1 Broken Access Control	**Last Time Tested**	11 Feb 2024 21:02 GMT+0200
WASC	WASC-15 APPLICATION MISCONFIGURATION WASC-16 DIRECTORY INDEXING WASC-17 IMPROPER FILESYSTEM PERMISSIONS	**Times Detected**	1

CVSS V3 Base	5.3	**CVSS V3 Temporal**	5	**CVSS V3 Attack Vector**	Network

Details

Threat
A file, directory, or directory listing was discovered on the Web server. These resources are confirmed to be present based on our logic. Some of the content on these files might have sensitive information.

NOTE: Links found in 150004 are found by forced crawling so will not automatically be added to 150009 Links Crawled or the application site map. If links found in 150004 need to be tested they must be added as Explicit URI so they are included in scope and then will be reported in 150009. Once the link is added to be in scope (i.e. Explicit URI) this same link will no longer be reported for 150004.

Impact
The contents of this file or directory may disclose sensitive information.

Solution
It is advised to review the contents of the disclosed files. If the contents contain sensitive information, please verify that access to this file or directory is permitted. If necessary, remove it or apply access controls to it.

Detection Information

Parameter	No param has been required for detecting the information.
Authentication	In order to detect this vulnerability, no authentication has been required.
Access Path	Here is the path followed by the scanner to reach the exploitable URL:

https://archibus.vodacom.co.za/fpr/index.asp
https://archibus.vodacom.co.za/Leasure-the-deed-will-the-clipt-Angely-ands-Banq

Payloads

#1 Request

GET https://archibus.vodacom.co.za/docs/config/download/

Referer: https://archibus.vodacom.co.za/fpr/index.asp
Cookie: visid_incap_2776849=XzGtDabQTHuVkbHOgCNGXPUZyWUAAAAAQUIPAAAAAABzHTfqgLA/hAMNNToBRAEF; nlbi_2776849_2147483392=/WJ+ATMjWG2jrQ/lZU49BAAAAACZlY7MnB6gaJItNr8GkCYJ; nlbi_2776849=1uvTSns0kGzwA8rXZU49BAAAAABumPnVc6r7kZo+kAK6WiUr; incap_ses_1687_2776849=ArRnARTRdWEO7PgfvG1pF/UZyWUAAAAACho9ich3SZo+8LGHMtIyTQ==;
Host: archibus.vodacom.co.za
User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/102.0.5005.177 Safari/537.36
Accept: */*

Click this link to try to reproduce the vulnerability using above payload.Note that clicking this link may not lead to visible results, either because the vulnerability requires context to be previously set (authentication, cookies...) or because the exploitation of the vulnerability does not lead to any visible proof.

#1 Response

comment:
Original URL is: https://archibus.vodacom.co.za/docs/config/

HTTP/1.1 200 OK

Information Disclosure (6)

150755 Apache Tomcat Request Smuggling Vulnerability (CVE-2023-46589) (1)

150755 Apache Tomcat Request Smuggling Vulnerability (CVE-2023-46589) *archibus.vodacom.co.za:443/fpr/index.asp* **New**

URL: https://archibus.vodacom.co.za/Tr7l6y8G.1tmhl

Finding #	23855526	**Severity**	Potential Vulnerability - Level 4
Unique #	08f0650d-d6ab-442b-995a-d5a41b592548		
Group	Information Disclosure	**First Time Detected**	11 Feb 2024 21:02 GMT+0200
CWE	CWE-444	**Last Time Detected**	11 Feb 2024 21:02 GMT+0200
OWASP	A4 Insecure Design	**Last Time Tested**	11 Feb 2024 21:02 GMT+0200
WASC	WASC-26 HTTP REQUEST SMUGGLING	**Times Detected**	1
CVSS V3 Base	7.5	**CVSS V3 Temporal**	6.5
CVSS V3 Attack Vector	Network		

Details

Threat

WAS Web Application Report

Apache Tomcat is an open source web server and servlet container developed by the Apache Software Foundation.

Tomcat did not correctly parse HTTP trailer headers. A specially crafted trailer header that exceeded the header size limit could cause Tomcat to treat a single request as multiple requests leading to the possibility of request smuggling when behind a reverse proxy.

Affected Versions:
Apache Tomcat 11.0.0-M1 to 11.0.0-M10
Apache Tomcat 10.1.0-M1 to 10.1.15
Apache Tomcat 9.0.0-M1 to 9.0.82
Apache Tomcat 8.5.0 to 8.5.95

QID Detection Logic (Unauthenticated):
This QID sends a HTTP GET request to a invalid URL and based on the response confirms the vulnerable instance of Apache Tomcat running on the host.

Impact

Exploitation of the vulnerability could lead to HTTP request smuggling attack.

Solution

Customers are advised to upgrade relevant versions of Apache Tomcat:
Apache Tomcat 11.0.0-M11 or later
Apache Tomcat 10.1.16 or later
Apache Tomcat 9.0.83 or later
Apache Tomcat 8.5.96 or later
For more information on this vulnerability please refer Apache Tomcat 8 Security Advisory, Apache Tomcat 9 Security Advisory, Apache Tomcat 10 Security Advisory, Apache Tomcat 11 Security Advisory.

Detection Information

Parameter	No param has been required for detecting the information.
Authentication	In order to detect this vulnerability, no authentication has been required.

Payloads

#1 Request

GET https://archibus.vodacom.co.za/Tr7l6y8G.1tmhl

Referer: https://archibus.vodacom.co.za/fpr/index.asp
Cookie: visid_incap_2776849=qLvFr0MgQVGyXYoa1Xr/T90syWUAAAAAQUIPAAAAAAAVqeFEBNtXCvYRcEoSpUQj; incap_ses_1687_2776849=b+blRcUfUUTd1xQgvG1pF90syWUAAAAAXWaR1GkQ9AjVBOa0Cp1jBQ==;
Host: archibus.vodacom.co.za
User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/102.0.5005.177 Safari/537.36
Accept: */*

Click this link to try to reproduce the vulnerability using above payload.Note that clicking this link may not lead to visible results, either because the vulnerability requires context to be previously set (authentication, cookies...) or because the exploitation of the vulnerability does not lead to any visible proof.

#1 Response

comment: Apache Tomcat Request Smuggling Vulnerability (CVE-2023-46589) found at PORT : 443

he requested resource [/Tr7l6y8G.1tmhl] is not available Description The origin server did not find a current representation for the target resource or is not willing to disclose that one exists. <hr class="line" /><h3>Apache Tomcat/9.0.62</h3><script type="text/javascript" src="/_Incapsula_Resource?SWJIYLWA=719d34d31c8e3a6e6fffd425f7e032f3&ns=1&cb=1052176229" async></script></body></html>

* The reflected string on the response webpage indicates that the vulnerability test was successful

150704 Apache Tomcat Open Redirect Vulnerability (CVE-2023-41080) (1)

150704 Apache Tomcat Open Redirect — *archibus.vodacom.co.za:443/fpr/index.asp* **New**

WAS Web Application Report

Vulnerability (CVE-2023-41080)

URL: https://archibus.vodacom.co.za/Bk3Xx8y2.1tmhl

Finding #	23855528	**Severity**	Potential Vulnerability - Level 3
Unique #	5066190c-4227-42c5-9a25-da44cc89e8af		
Group	Information Disclosure	**First Time Detected**	11 Feb 2024 21:02 GMT+0200
CWE	CWE-601	**Last Time Detected**	11 Feb 2024 21:02 GMT+0200
OWASP	A3 Injection	**Last Time Tested**	11 Feb 2024 21:02 GMT+0200
WASC	WASC-38 URL REDIRECTOR ABUSE	**Times Detected**	1

CVSS V3 Base	6.1	**CVSS V3 Temporal**	5.3	**CVSS V3 Attack Vector**	Network

Details

Threat

Apache Tomcat is an open source web server and servlet container developed by the Apache Software Foundation.

If the ROOT (default) web application is configured to use FORM authentication then it is possible that a specially crafted URL could be used to trigger a redirect to an URL of the attackers choice.

Affected Versions:
Apache Tomcat 11.0.0-M1 to 11.0.0-M10
Apache Tomcat 10.1.0-M1 to 10.1.12
Apache Tomcat 9.0.0-M1 to 9.0.79
Apache Tomcat 8.5.0 to 8.5.92

QID Detection Logic (Unauthenticated):
This QID sends a HTTP GET request to a invalid URL and based on the response confirms the vulnerable instance of Apache Tomcat running on the host.

Impact

Successful exploitation could allow attackers to trick a user into visiting a specially crafted link which would redirect them to an arbitrary malicious external URL.

Solution

To address this vulnerability, it is recommended that customers upgrade to one of the following versions of Apache Tomcat: 11.0.0-M11, 10.1.13, 9.0.80, or 8.5.93, or install a newer version. For additional information, please refer to the Apache Tomcat Security Advisory.

Detection Information

Parameter	No param has been required for detecting the information.
Authentication	In order to detect this vulnerability, no authentication has been required.

Payloads

WAS Web Application Report

#1 Request

GET https://archibus.vodacom.co.za/Bk3Xx8y2.1tmhl

Referer: https://archibus.vodacom.co.za/fpr/index.asp
Cookie: visid_incap_2776849=QqkI6U3ET0iook9FZcNy5kMryWUAAAAAQUIPAAAAAAC2mYEiORY8E6pWpcdDyixM; incap_ses_1687_2776849=k/CCUPZFaB4PWRIgvG1pF0MryWUAAAAAsA5YA/1RDlktNgosdk5tGQ==;
Host: archibus.vodacom.co.za
User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/102.0.5005.177 Safari/537.36
Accept: */*

Click this link to try to reproduce the vulnerability using above payload.Note that clicking this link may not lead to visible results, either because the vulnerability requires context to be previously set (authentication, cookies...) or because the exploitation of the vulnerability does not lead to any visible proof.

#1 Response

comment: Apache Tomcat Open Redirect Vulnerability (CVE-2023-41080) found at PORT : 443

he requested resource [/Bk3Xx8y2.1tmhl] is not available Description The origin server did not find a current representation for the target resource or is not willing to disclose that one exists. <hr class="line" /><h3>Apache Tomcat/9.0.62</h3><script type="text/javascript" src="/_Incapsula_Resource?SWJIYLWA=719d34d31c8e3a6e6fffd425f7e032f3&ns=1&cb=1706438915" async></script></body></html>

* The reflected string on the response webpage indicates that the vulnerability test was successful

150122 Cookie Does Not Contain The "secure" Attribute (1)

150122 Cookie Does Not Contain The "secure" Attribute — *archibus.vodacom.co.za:443/fpr/index.asp* **Active**

URL: https://archibus.vodacom.co.za/fpr/index.asp

Finding #	18390526	**Severity**	Confirmed Vulnerability - Level 2
Unique #	547dbba6-6006-45eb-b522-281c87f57687		
Group	Information Disclosure	**First Time Detected**	22 Jan 2023 21:25 GMT+0200
CWE	CWE-614	**Last Time Detected**	11 Feb 2024 21:02 GMT+0200
OWASP	A5 Security Misconfiguration	**Last Time Tested**	11 Feb 2024 21:02 GMT+0200
WASC	WASC-4 INSUFFICIENT TRANSPORT LAYER PROTECTION	**Times Detected**	15
CVSS V3 Base	4.3	**CVSS V3 Temporal**	4.1
CVSS V3 Attack Vector	Network		

Details

Threat
The cookie does not contain the "secure" attribute.

Impact
Cookies with the "secure" attribute are only permitted to be sent via HTTPS. Cookies sent via HTTP expose an unsuspecting user to sniffing attacks that could lead to user impersonation or compromise of the application account.

Solution
If the associated risk of a compromised account is high, apply the "secure" attribute to cookies and force all sensitive requests to be sent via HTTPS.

Detection Information

Cookie Name(s)	**visid_incap_2776849, incap_ses_1687_2776849, nlbi_2776849, nlbi_2776849_2147483392**
Authentication	In order to detect this vulnerability, no authentication has been required.

Payloads

WAS Web Application Report

#1 Request

GET https://archibus.vodacom.co.za/fpr/index.asp

Host: archibus.vodacom.co.za
User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/102.0.5005.177 Safari/537.36
Accept: */*

Click this link to try to reproduce the vulnerability using above payload.Note that clicking this link may not lead to visible results, either because the vulnerability requires context to be previously set (authentication, cookies...) or because the exploitation of the vulnerability does not lead to any visible proof.

#1 Response

visid_incap_2776849=
H2 404
content-encoding: gzip
content-security-policy-report-only: default-src 'self' 'unsafe-eval' 'unsafe-hashes' 'unsafe-inline' data: blob: ; form-action 'none' data: blob: ; report-uri /csp_report
content-type: text/html
date: Sun, 11 Feb 2024 19:03:18 GMT
instance: /ITG/pool_archibus_8080 10.134.16.81 8080
server: Microsoft-IIS/10.0
set-cookie: visid_incap_2776849=XzGtDabQTHuVkbHOgCNGXPUZyWUAAAAAQUIPAAAAAABzHTfqgLA/hAMNNToBRAEF; expires=Sun, 09 Feb 2025 22:21:09 GMT; HttpOnly; path=/; Domain=.vodacom.co.za
nlbi_2776849=1uvTSns0kGzwA8rXZU49BAAAAABumPnVc6r7kZo+kAK6WiUr; path=/; Domain=.vodacom.co.za
incap_ses_1687_2776849=ArRnARTRdWEO7PgfvG1pF/UZyWUAAAAACho9ich3SZo+8LGHMtIyTQ==; path=/; Domain=.vodacom.co.za
x-cdn: Imperva
x-frame-options: SAMEORIGIN
x-iinfo: 62-26458618-26458621 NNYY CT(164 164 0) RT(1707678197609 22) q(0 0 0 -1) r(1 1) U11
x-powered-by: ASP.NET

incap_ses_1687_2776849=
H2 404
content-encoding: gzip
content-security-policy-report-only: default-src 'self' 'unsafe-eval' 'unsafe-hashes' 'unsafe-inline' data: blob: ; form-action 'none' data: blob: ; report-uri /csp_report
content-type: text/html
date: Sun, 11 Feb 2024 19:03:18 GMT
instance: /ITG/pool_archibus_8080 10.134.16.81 8080
server: Microsoft-IIS/10.0
set-cookie: visid_incap_2776849=XzGtDabQTHuVkbHOgCNGXPUZyWUAAAAAQUIPAAAAAABzHTfqgLA/hAMNNToBRAEF; expires=Sun, 09 Feb 2025 22:21:09 GMT; HttpOnly; path=/; Domain=.vodacom.co.za
nlbi_2776849=1uvTSns0kGzwA8rXZU49BAAAAABumPnVc6r7kZo+kAK6WiUr; path=/; Domain=.vodacom.co.za
incap_ses_1687_2776849=ArRnARTRdWEO7PgfvG1pF/UZyWUAAAAACho9ich3SZo+8LGHMtIyTQ==; path=/; Domain=.vodacom.co.za
x-cdn: Imperva
x-frame-options: SAMEORIGIN
x-iinfo: 62-26458618-26458621 NNYY CT(164 164 0) RT(1707678197609 22) q(0 0 0 -1) r(1 1) U11
x-powered-by: ASP.NET

nlbi_2776849=
H2 404
content-encoding: gzip
content-security-policy-report-only: default-src 'self' 'unsafe-eval' 'unsafe-hashes' 'unsafe-inline' data: blob: ; form-action 'none' data: blob: ; report-uri /csp_report
content-type: text/html
date: Sun, 11 Feb 2024 19:03:18 GMT
instance: /ITG/pool_archibus_8080 10.134.16.81 8080
server: Microsoft-IIS/10.0
set-cookie: visid_incap_2776849=XzGtDabQTHuVkbHOgCNGXPUZyWUAAAAAQUIPAAAAAABzHTfqgLA/hAMNNToBRAEF; expires=Sun, 09 Feb 2025 22:21:09 GMT; HttpOnly; path=/; Domain=.vodacom.co.za
nlbi_2776849=1uvTSns0kGzwA8rXZU49BAAAAABumPnVc6r7kZo+kAK6WiUr; path=/; Domain=.vodacom.co.za
incap_ses_1687_2776849=ArRnARTRdWEO7PgfvG1pF/UZyWUAAAAACho9ich3SZo+8LGHMtIyTQ==; path=/; Domain=.vodacom.co.za
x-cdn: Imperva
x-frame-options: SAMEORIGIN
x-iinfo: 62-26458618-26458621 NNYY CT(164 164 0) RT(1707678197609 22) q(0 0 0 -1) r(1 1) U11
x-powered-by: ASP.NET

nlbi_2776849_2147483392=
H2 200
access-control-allow-origin: *
cache-control: max-age=60
content-encoding: gzip
content-length: 77738
content-security-policy-report-only: default-src 'self' 'unsafe-eval' 'unsafe-hashes' 'unsafe-inline' data: blob: ; form-action 'none' data: blob: ; report-uri /csp_report
content-type: text/javascript
date: Sun, 11 Feb 2024 19:03:18 GMT
server: bon
server-timing: bon, total;dur=10.636971
set-cookie: nlbi_2776849_2147483392=a6JeKHL+xgNWhQdiZU49BAAAAABtrQ53JjbMXz9smE8uFxJx; path=/; Domain=.vodacom.co.za
x-cdn: Imperva
x-iinfo: 62-26458618-26458659 NNNN CT(9 9 0) RT(1707678197609 335) q(0 0 0 0) r(0 0) U18

150123 Cookie Does Not Contain The "HTTPOnly" Attribute (1)

WAS Web Application Report

150123 Cookie Does Not Contain The "HTTPOnly" Attribute

archibus.vodacom.co.za:443/fpr/index.asp **Active**

URL: https://archibus.vodacom.co.za/fpr/index.asp

Finding #	18390528	**Severity**	Confirmed Vulnerability - Level 2
Unique #	3fc377f4-8f67-4e01-9a3b-df3edf436316		
Group	Information Disclosure	**First Time Detected**	22 Jan 2023 21:25 GMT+0200
CWE	CWE-1004	**Last Time Detected**	11 Feb 2024 21:02 GMT+0200
OWASP	A5 Security Misconfiguration	**Last Time Tested**	11 Feb 2024 21:02 GMT+0200
WASC	WASC-4 INSUFFICIENT TRANSPORT LAYER PROTECTION	**Times Detected**	15

CVSS V3 Base	4.3	**CVSS V3 Temporal**	4.1	**CVSS V3 Attack Vector**	Network

Details

Threat

The cookie does not contain the "HTTPOnly" attribute.

Impact

Cookies without the "HTTPOnly" attribute are permitted to be accessed via JavaScript. Cross-site scripting attacks can steal cookies which could lead to user impersonation or compromise of the application account.

Solution

If the associated risk of a compromised account is high, apply the "HTTPOnly" attribute to cookies.

Detection Information

Cookie Name(s)	**nlbi_2776849_2147483392, incap_ses_1687_2776849, nlbi_2776849**
Authentication	In order to detect this vulnerability, no authentication has been required.

Payloads

#1 Request

GET https://archibus.vodacom.co.za/fpr/index.asp

Host: archibus.vodacom.co.za
User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/102.0.5005.177 Safari/537.36
Accept: */*

Click this link to try to reproduce the vulnerability using above payload.Note that clicking this link may not lead to visible results, either because the vulnerability requires context to be previously set (authentication, cookies...) or because the exploitation of the vulnerability does not lead to any visible proof.

#1 Response

nlbi_2776849_2147483392=
H2 200
access-control-allow-origin: *
cache-control: max-age=60
content-encoding: gzip
content-length: 77738
content-security-policy-report-only: default-src 'self' 'unsafe-eval' 'unsafe-hashes' 'unsafe-inline' data: blob: ; form-action 'none' data: blob: ; report-uri /csp_report
content-type: text/javascript
date: Sun, 11 Feb 2024 19:03:18 GMT
server: bon
server-timing: bon, total;dur=10.636971
set-cookie: nlbi_2776849_2147483392=a6JeKHL+xgNWhQdiZU49BAAAAABtrQ53JjbMXz9smE8uFxJx; path=/; Domain=.vodacom.co.za
x-cdn: Imperva
x-iinfo: 62-26458618-26458659 NNNN CT(9 9 0) RT(1707678197609 335) q(0 0 0 0) r(0 0) U18

incap_ses_1687_2776849=
H2 404
content-encoding: gzip
content-security-policy-report-only: default-src 'self' 'unsafe-eval' 'unsafe-hashes' 'unsafe-inline' data: blob: ; form-action 'none' data: blob: ; report-uri /csp_report
content-type: text/html
date: Sun, 11 Feb 2024 19:03:18 GMT
instance: /ITG/pool_archibus_8080 10.134.16.81 8080
server: Microsoft-IIS/10.0
set-cookie: visid_incap_2776849=XzGtDabQTHuVkbHOgCNGXPUZyWUAAAAAQUIPAAAAAABzHTfqgLA/hAMNNToBRAEF; expires=Sun, 09 Feb 2025 22:21:09 GMT; HttpOnly; path=/; Domain=.vodacom.co.za
nlbi_2776849=1uvTSns0kGzwA8rXZU49BAAAAABumPnVc6r7kZo+kAK6WiUr; path=/; Domain=.vodacom.co.za
incap_ses_1687_2776849=ArRnARTRdWEO7PgfvG1pF/UZyWUAAAAACho9ich3SZo+8LGHMtIyTQ==; path=/; Domain=.vodacom.co.za
x-cdn: Imperva
x-frame-options: SAMEORIGIN
x-iinfo: 62-26458618-26458621 NNYY CT(164 164 0) RT(1707678197609 22) q(0 0 0 -1) r(1 1) U11
x-powered-by: ASP.NET

nlbi_2776849=
H2 404
content-encoding: gzip
content-security-policy-report-only: default-src 'self' 'unsafe-eval' 'unsafe-hashes' 'unsafe-inline' data: blob: ; form-action 'none' data: blob: ; report-uri /csp_report
content-type: text/html
date: Sun, 11 Feb 2024 19:03:18 GMT
instance: /ITG/pool_archibus_8080 10.134.16.81 8080
server: Microsoft-IIS/10.0
set-cookie: visid_incap_2776849=XzGtDabQTHuVkbHOgCNGXPUZyWUAAAAAQUIPAAAAAABzHTfqgLA/hAMNNToBRAEF; expires=Sun, 09 Feb 2025 22:21:09 GMT; HttpOnly; path=/; Domain=.vodacom.co.za
nlbi_2776849=1uvTSns0kGzwA8rXZU49BAAAAABumPnVc6r7kZo+kAK6WiUr; path=/; Domain=.vodacom.co.za
incap_ses_1687_2776849=ArRnARTRdWEO7PgfvG1pF/UZyWUAAAAACho9ich3SZo+8LGHMtIyTQ==; path=/; Domain=.vodacom.co.za
x-cdn: Imperva
x-frame-options: SAMEORIGIN
x-iinfo: 62-26458618-26458621 NNYY CT(164 164 0) RT(1707678197609 22) q(0 0 0 -1) r(1 1) U11
x-powered-by: ASP.NET

150476 Cookies Issued Without User Consent (1)

150476 Cookies Issued Without User Consent — *archibus.vodacom.co.za:443/fpr/index.asp* **Active**

URL: https://archibus.vodacom.co.za/fpr/index.asp

Finding #	18390524	**Severity**	Confirmed Vulnerability - Level 2
Unique #	639e3050-d191-474d-9a77-354f4ffdc294		
Group	Information Disclosure	**First Time Detected**	22 Jan 2023 21:25 GMT+0200
CWE	CWE-565	**Last Time Detected**	11 Feb 2024 21:02 GMT+0200
OWASP	A5 Security Misconfiguration	**Last Time Tested**	11 Feb 2024 21:02 GMT+0200
WASC	-	**Times Detected**	15

CVSS V3 Base 5.3 **CVSS V3 Temporal** 4.5 **CVSS V3 Attack Vector** Network

WAS Web Application Report

Details

Threat
The cookies listed in the Results section were issued from the web application during the crawl without accepting any opt-in dialogs.

Impact
Cookies may be set without user explicitly agreeing to accept them.

Solution
Review the application to ensure that all cookies listed are supposed to be issued without user opt-in. If the EU Cookie law is applicable for this web application, ensure these cookies require user opt-in or have been classified as exempt by your organization.

Detection Information

Parameter	No param has been required for detecting the information.
Authentication	In order to detect this vulnerability, no authentication has been required.

Payloads

#1 Request

GET https://archibus.vodacom.co.za/fpr/index.asp

Host: archibus.vodacom.co.za
User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/102.0.5005.177 Safari/537.36
Accept: */*

Click this link to try to reproduce the vulnerability using above payload.Note that clicking this link may not lead to visible results, either because the vulnerability requires context to be previously set (authentication, cookies...) or because the exploitation of the vulnerability does not lead to any visible proof.

#1 Response

Total cookies: 4
nlbi_2776849=L17kcRBaa3GJaFCEZU49BAAAAADqWKWqShXnjWNONnOBMlpx; domain=.vodacom.co.za; path=/ First set at URL: https://archibus.vodacom.co.za/_Incapsula_Resource?SWJIYLWA=719d34d31c8e3a6e6fffd425f7e032f3%22ns=84%22cb=1882006911
visid_incap_2776849=K/6dnS2TRqa+OIWNcorGK7EpyWUAAAAAQUIPAAAAAAAyOyOsWlSi79JS1yDHHk81; HttpOnly; expires=Sun, 09-Feb-2025 22:21:09 GMT; domain=.vodacom.co.za; path=/ First set at URL: https://archibus.vodacom.co.za/_Incapsula_Resource?SWJIYLWA=719d34d31c8e3a6e6fffd425f7e032f3%22ns=84%22cb=1882006911
incap_ses_1687_2776849=6hmvUMCXIlti2A8gvG1pF7EpyWUAAAAAtuWs1PpyWy19fX6IBJSYzA==; domain=.vodacom.co.za; path=/ First set at URL: https://archibus.vodacom.co.za/_Incapsula_Resource?SWJIYLWA=719d34d31c8e3a6e6fffd425f7e032f3%22ns=84%22cb=1882006911
nlbi_2776849_2147483392=vUrgCHopZwFLJfwBZU49BAAAAADSVQcwEjLPgbvVb6G6Ox2O; domain=.vodacom.co.za; path=/ First set at URL: https://archibus.vodacom.co.za/_Incapsula_Resource?SWJIYLWA=719d34d31c8e3a6e6fffd425f7e032f3%22ns=84%22cb=1882006911

150630 CORS header misconfigured (1)

150630 CORS header misconfigured — *archibus.vodacom.co.za:443/fpr/index.asp* **Active**

URL: https://archibus.vodacom.co.za/Leasure-the-deed-will-the-clipt-Angely-ands-Banq?d=archibus.vodacom.co.za

Finding #	19053724	**Severity**	Potential Vulnerability - Level 1
Unique #	5c5a4e42-7159-463c-9f12-e3ed4bf93a6b		
Group	Information Disclosure	**First Time Detected**	17 Mar 2023 00:13 GMT+0200
CWE	CWE-942	**Last Time Detected**	11 Feb 2024 21:02 GMT+0200
OWASP	A5 Security Misconfiguration	**Last Time Tested**	11 Feb 2024 21:02 GMT+0200
WASC	-	**Times Detected**	14

CVSS V3 Base	4.3	**CVSS V3 Temporal**	4	**CVSS V3 Attack Vector**	Network

Details

WAS Web Application Report

Threat

Cross-Origin Resource Sharing (CORS) is an HTTP-header based mechanism that allows a server to indicate any origins (domain, scheme, or port) other than its own from which a browser should permit loading resources. CORS also relies on a mechanism by which browsers make a "preflight" request to the server hosting the cross-origin resource, in order to check that the server will permit the actual request. In that preflight, the browser sends headers that indicate the HTTP method and headers that will be used in the actual request. For security reasons, browsers restrict cross-origin HTTP requests initiated from scripts. The "Access-Control-Allow-Origin" header is used to specify the allowed origins to access the resource.

The WAS scanning engine detects the vulnerability by examining the "Access-Control-Allow-Origin" header for a wildcard value (*). This value in the response to an XHR request indicate that the resource can be accessed from any domain and needs to be strictly configured.

Impact

If CORS is misconfigured, it can lead to major security risk like access to sensitive data, API keys and other users' data from any domain. This access could lead to misuse and exploitation of protected resource.

Solution

CORS header misconfiguration can be addressed by providing only the list of allowed domains in the "Access-Control-Allow-Origin" header. The wildcard character (*) should never be provided as it indicates any domain can access the resource.

Detection Information

Parameter	No param has been required for detecting the information.
Authentication	In order to detect this vulnerability, no authentication has been required.
Access Path	Here is the path followed by the scanner to reach the exploitable URL:

https://archibus.vodacom.co.za/fpr/index.asp

Payloads

#1 Request

POST https://archibus.vodacom.co.za/Leasure-the-deed-will-the-clipt-Angely-ands-Banq? d=archibus.vodacom.co.za

Origin: http://azbycxdwev.com
Referer: https://archibus.vodacom.co.za/fpr/index.asp
Cookie: visid_incap_2776849=XzGtDabQTHuVkbHOgCNGXPUZyWUAAAAAQUIPAAAAAABzHTfqgLA/hAMNNToBRAEF; nlbi_2776849_2147483392=/WJ+ATMjWG2jrQ/lZU49BAAAAACZlY7MnB6gaJItNr8GkCYJ; nlbi_2776849=1uvTSns0kGzwA8rXZU49BAAAAABumPnVc6r7kZo+kAK6WiUr; incap_ses_1687_2776849=ArRnARTRdWEO7PgfvG1pF/UZyWUAAAAACho9ich3SZo+8LGHMtIyTQ==;
Host: archibus.vodacom.co.za
User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/102.0.5005.177 Safari/537.36
Accept: */*
Content-Type: application/x-www-form-urlencoded

-

Click this link to try to reproduce the vulnerability using above payload.Note that clicking this link may not lead to visible results, either because the vulnerability requires context to be previously set (authentication, cookies...) or because the exploitation of the vulnerability does not lead to any visible proof.

#1 Response

comment: CORS header Access-Control-Allow-Origin is misconfigured or is too permissive.

Response headers:
access-control-allow-origin: *
server-timing: bon, total;dur=0.042929999999999996
server: bon
keep-alive: timeout=60
content-length: 0
date: Sun, 11 Feb 2024 19:52:46 GMT
Set-Cookie: nlbi_2776849_2147483392=QlCESNC4InbI3BQfZU49BAAAAADGNtJNp9ntQPPFg5UpjNRq; path=/; Domain=.vodacom.co.za
Set-Cookie: incap_ses_1687_2776849=jpIgGh+8qyfPlAcgvG1pF40lyWUAAAAAii/ne4vzkdfBRsI++YFQkA==; path=/; Domain=.vodacom.co.za
X-CDN: Imperva
Content-Security-Policy-Report-Only: default-src 'self' 'unsafe-eval' 'unsafe-hashes' 'unsafe-inline' data: blob: ; form-action 'none' data: blob: ; report-uri /csp_report
X-Iinfo: 24-5715943-5715940 PNNN RT(1707681165943 2) q(0 0 0 0) r(0 0) U6

WAS Web Application Report

Information Gathered (41)

Information Gathered (1)

150497 Progressive scan completely crawled and tested the website (1)

150497 Progressive scan completely crawled and tested the website

archibus.vodacom.co.za:443/fpr/index.as

Finding #	10974624	**Severity**	Information Gathered - Level 1
Unique #	b5c59f16-576a-4a06-bfbb-de4be1ec8f4c		
Group	Information Gathered		
CWE	-	**Detection Date**	11 Feb 2024 21:02 GMT+0200
OWASP	-		
WASC	-		

Details

Threat

Scan covered the whole scope of the web application and finished all test phases.
QID is reported, starting from progression 2. When progression 1 is launched and scan is finished it is considered as single scan, hence QID will not be reported.
If subsequent scans are completed with all phases QID 150497 will be reported.

Impact

N/A

Solution

Review QID 150021 for additional details of phases completed during this scan.

Results

Scan covered the whole scope of the web application and finished all test phases.

Scan Diagnostics (26)

150018 Connection Error Occurred During Web Application Scan (1)

150018 Connection Error Occurred During Web Application Scan

archibus.vodacom.co.za:443/fpr/index.as

Finding #	10541619	**Severity**	Information Gathered - Level 2
Unique #	dd6eaedf-925c-434f-93e0-9f3e25874c2b		
Group	Scan Diagnostics		
CWE	-	**Detection Date**	11 Feb 2024 21:02 GMT+0200
OWASP	-		
WASC	-		

Details

Threat

The following are some of the possible reasons for the timeouts or connection errors:
1. A disturbance in network connectivity between the scanner and the web application occurred.
2. The web server or application server hosting the application was taken down in the midst of a scan.
3. The web application experienced an overload, possibly due to load generated by the scan.
4. An error occurred in the SSL/TLS handshake (applies to HTTPS web applications only).
5. A security device, such as an IDS/IPS or web application firewall (WAF), began to drop or reject the HTTP connections from the scanner.
6. Very large files like PDFs, videos, etc. are present on the site and caused timeouts when accessed by the scanner.

Impact

Some of the links were not crawled or scanned. Results may be incomplete or incorrect.

Solution

First, confirm that the server was not taken down in the midst of the scan. After that, investigate the root cause by reviewing the listed links and examining web server logs, application server logs, or IDS/IPS/WAF logs. If the errors are caused due to load generated by the scanner then try reducing the scan intensity (this could increase the scan duration). If the errors are due to specific URLs being tested by the scanner or due to specific form data sent by the scanner, then configure exclude lists in the scan configuration as needed to avoid such requests. If timeouts or connection errors are a persistent issue but you want the scan to run to completion, change the Behavior Settings in the option profile to increase the error thresholds or disable the error checks entirely.

Results

Total number of unique links that encountered timeout errors: 54
Links with highest number of timeouts:
11 https://archibus.vodacom.co.za/
7 https://archibus.vodacom.co.za/docs/
7 https://archibus.vodacom.co.za/fpr/
3 https://archibus.vodacom.co.za/Leasure-the-deed-will-the-clipt-Angely-ands-Banq?d=archibus.vodacom.co.za
2 https://archibus.vodacom.co.za/FPRWin/
1 https://archibus.vodacom.co.za/docs/api/service.asmx?wsdl
1 https://archibus.vodacom.co.za/_Incapsula_Resource?CWUDNSAI=23&xinfo=1-22384977-0%200NNN%20RT%2816998157090 16%2016037%29%20q%280%20-1%20-1%200%29%20r%280%20-1%29%20B15%284%2C200%2C0%29%20U18&incident_id=%22'%3E%3Cqss%20a%3DX47442512Y3_1Z%3E&edet=15&cinfo=04000000&rpinfo=0&mth=GET
1 https://archibus.vodacom.co.za/FPRWin/index.aspx
1 https://archibus.vodacom.co.za/_Incapsula_Resource?CWUDNSAI=23&xinfo=1-22384977-0%200NNN%20RT%2816998157090 16%2016037%29%20q%280%20-1%20-1%200%29%20r%280%20-1%29%20B15%284%2C200%2C0%29%20U18&incident_id=%00%3Cscript%3E_q%3Drandom(X47442512Y3_1Z)%3C%2Fscript%3E&edet=15&cinfo=04000000&rpinfo=0&mth=GET
1 https://archibus.vodacom.co.za/api.asmx?wsdl
1 https://archibus.vodacom.co.za/docs/appdev/service.asmx?wsdl
1 https://archibus.vodacom.co.za/_Incapsula_Resource?SWKMTFSR=%22'%3E%3Cqss%20a%3DX139942785521904Y1_1Z%3E&e=0.11641625286643564
1 https://archibus.vodacom.co.za/_Incapsula_Resource?CWUDNSAI=23&xinfo=1-22384977-0%200NNN%20RT%2816998157090 16%2016037%29%20q%280%20-1%20-1%200%29%20r%280%20-1%29%20B15%284%2C200%2C0%29%20U18&incident_id=767000500460857534-122447288571202689&edet=15&cinfo=%22'%3E%3Cqss%20a%3DX47442512Y5_1Z%3E&rpinfo=0&mth=GET
1 https://archibus.vodacom.co.za/fpr/api.asmx?wsdl
1 https://archibus.vodacom.co.za/docs/config/ws.asmx?wsdl
1 https://archibus.vodacom.co.za/manager/service.asmx?wsdl
1 https://archibus.vodacom.co.za/_Incapsula_Resource?CWUDNSAI=23&xinfo=1-22384977-0%200NNN%20RT%2816998157090 16%2016037%29%20q%280%20-1%20-1%200%29%20r%280%20-1%29%20B15%284%2C200%2C0%29%20U18&incident_id=767000500460857534-122447288571202689&edet=15&cinfo=04000000&rpinfo=0&mth=%22'%3E%3Cqss%20a%3DX47442512Y7_1Z%3E
1 https://archibus.vodacom.co.za/_Incapsula_Resource?CWUDNSAI=%22'%3E%3Cqss%20a%3DX47442512Y1_1Z%3E&xinfo=1-22384977-0%200NNN%20RT%2816998157090 16%2016037%29%20q%280%20-1%20-1%200%29%20r%280%20-1%29%20B15%284%2C200%2C0%29%20U18&incident_id=767000500460857534-122447288571202689&edet=15&cinfo=04000000&rpinfo=0&mth=GET
1 https://archibus.vodacom.co.za/examples/
1 https://archibus.vodacom.co.za/docs/api.asmx?wsdl
1 https://archibus.vodacom.co.za/FPRWin/api.asmx?wsdl
1 https://archibus.vodacom.co.za/docs/appdev/api.asmx?wsdl
1 https://archibus.vodacom.co.za/docs/ws.asmx?wsdl
1 https://archibus.vodacom.co.za/docs/api/api.asmx?wsdl
1 https://archibus.vodacom.co.za/docs/realm-howto.html
1 https://archibus.vodacom.co.za/fpr/ws.asmx?wsdl
1 https://archibus.vodacom.co.za/_Incapsula_Resource?CWUDNSAI=23&xinfo=%22'%3E%3Cqss%20a%3DX47442512Y2_1Z%3E&incident_id=767000500460857534-122447288571202689&edet=15&cinfo=04000000&rpinfo=0&mth=GET
1 https://archibus.vodacom.co.za/service.asmx?wsdl
1 https://archibus.vodacom.co.za/docs/service.asmx?wsdl
1 https://archibus.vodacom.co.za/_Incapsula_Resource?SWKMTFSR=%00%3Cscript%3E_q%3Drandom(X139942785521904Y1_1Z)%3C%2Fscript%3E&e=0.11641625286643564
1 https://archibus.vodacom.co.za/host-manager/service.asmx?wsdl
1 https://archibus.vodacom.co.za/_Incapsula_Resource?CWUDNSAI=23&xinfo=1-22384977-0%200NNN%20RT%2816998157090 16%2016037%29%20q%280%20-1%20-1%200%29%20r%280%20-1%29%20B15%284%2C200%2C0%29%20U18&incident_id=767000500460857534-122447288571202689&edet=15&cinfo=04000000&rpinfo=%22'%3E%3Cqss%20a%3DX47442512Y6_1Z%3E&mth=GET
1 https://archibus.vodacom.co.za/host-manager/WS/
1 https://archibus.vodacom.co.za/examples/service.asmx?wsdl
1 https://archibus.vodacom.co.za/ws.asmx?wsdl
1 https://archibus.vodacom.co.za/docs/RELEASE-NOTES.txt
1 https://archibus.vodacom.co.za/fpr/service.asmx?wsdl
1 https://archibus.vodacom.co.za/_Incapsula_Resource?CWUDNSAI=23&xinfo=1-22384977-0%200NNN%20RT%2816998157090 16%2016037%29%20q%280%20-1%20-1%200%29%20r%280%20-1%29%20B15%284%2C200%2C0%29%20U18&incident_id=767000500460857534-122447288571202689&edet=15&cinfo=%00%3Cscript%3E_q%3Drandom(X47442512Y5_1Z)%3C%2Fscript%3E&rpinfo=0&mth=GET
1 https://archibus.vodacom.co.za/docs/config/api.asmx?wsdl
1 https://archibus.vodacom.co.za/_Incapsula_Resource?SWKMTFSR=1&e=%00%3Cscript%3E_q%3Drandom(X139942785521904Y2_1Z)%3C%2Fscript%3E
1 https://archibus.vodacom.co.za/docs/config/service.asmx?wsdl
1 https://archibus.vodacom.co.za/_Incapsula_Resource?SWKMTFSR=1&e=%22'%3E%3Cqss%20a%3DX139942785521904Y2_1Z%3E
1 https://archibus.vodacom.co.za/docs/setup.html
1 https://archibus.vodacom.co.za/host-manager/api.asmx?wsdl
1 https://archibus.vodacom.co.za/_Incapsula_Resource?CWUDNSAI=%00%3Cscript%3E_q%3Drandom(X47442512Y1_1Z)%3C%2Fscript%3E&xinfo=1-22384977-0%200NNN%20RT%2816998157090 16%2016037%29%20q%280%20-1%20-1%200%29%20r%280%20-1%29%20B15%284%2C200%2C0%29%20U18&incident_id=767000500460857534-122447288571202689&edet=15&cinfo=04000000&rpinfo=0&mth=GET
1 https://archibus.vodacom.co.za/examples/api.asmx?wsdl
1 https://archibus.vodacom.co.za/_Incapsula_Resource?CWUDNSAI=23&xinfo=1-22384977-0%200NNN%20RT%2816998157090 16%2016037%29%20q%280%20-1%20-1%200%29%20r%280%20-1%29%20B15%284%2C200%2C0%29%20U18&incident_id=767000500460857534-122447288571202689&edet=%00%3Cscript%3E_q%3Drandom(X47442512Y4_1Z)%3C%2Fscript

%3E&cinfo=04000000&rpinfo=0&mth=GET
1 https://archibus.vodacom.co.za/_Incapsula_Resource?CWUDNSAI=23&xinfo=%00%3Cscript%3E_q%3Drandom(X47442512Y2_1Z)%3C%2Fscript%3E&incident_id=767000500460857534-122447288571202689&edet=15&cinfo=04000000&rpinfo=0&mth=GET
1 https://archibus.vodacom.co.za/examples/ws.asmx?wsdl
1 https://archibus.vodacom.co.za/docs/config/WebService/
1 https://archibus.vodacom.co.za/_Incapsula_Resource?CWUDNSAI=23&xinfo=1-22384977-0%200NNN%20RT%281699815709016%2016037%29%20q%280%20-1%20-1%200%29%20r%280%20-1%29%20B15%284%2C200%2C0%29%20U18&incident_id=767000500460857534-122447288571202689&edet=%22'%3E%3Cqss%20a%3DX47442512Y4_1Z%3E&cinfo=04000000&rpinfo=0&mth=GET
1 https://archibus.vodacom.co.za/FPRWin/service.asmx?wsdl
1 https://archibus.vodacom.co.za/manager/api.asmx?wsdl
1 https://archibus.vodacom.co.za/manager/ws.asmx?wsdl

Total number of unique links that encountered connection errors: 7
Links with highest number of connection errors:
1 https://archibus.vodacom.co.za/_Incapsula_Resource?SWKMTFSR=1&e='%20onEvent%3DX139942785521904Y2_1Z%20
1 https://archibus.vodacom.co.za/_Incapsula_Resource?SWKMTFSR='%20onEvent%3DX139942785521904Y1_1Z%20&e=0.11641625286643564
1 https://archibus.vodacom.co.za/_Incapsula_Resource?CWUDNSAI=23&xinfo=1-22384977-0%200NNN%20RT%281699815709016%2016037%29%20q%280%20-1%20-1%200%29%20r%280%20-1%29%20B15%284%2C200%2C0%29%20U18&incident_id=767000500460857534-122447288571202689&edet=15&cinfo=04000000&rpinfo=%00%3Cscript%3E_q%3Drandom(X47442512Y6_1Z)%3C%2Fscript%3E&mth=GET
1 https://archibus.vodacom.co.za/FPRWin/
1 https://archibus.vodacom.co.za/Leasure-the-deed-will-the-clipt-Angely-ands-Banq?d=archibus.vodacom.co.za
1 https://archibus.vodacom.co.za/fpr/null
1 https://archibus.vodacom.co.za/_Incapsula_Resource?CWUDNSAI=23&xinfo=1-22384977-0%200NNN%20RT%281699815709016%2016037%29%20q%280%20-1%20-1%200%29%20r%280%20-1%29%20B15%284%2C200%2C0%29%20U18&incident_id=767000500460857534-122447288571202689&edet=15&cinfo=04000000&rpinfo=0&mth=%00%3Cscript%3E_q%3Drandom(X47442512Y7_1Z)%3C%2Fscript%3E

Phase wise summary of timeout and connection errors encountered:
ePhaseWSDirectoryPathTests : 2 0
ePhaseWSEnumeration : 26 0
ePhaseParameterTests : 16 4
ePhaseWebCgiOob : 27 1
ePhaseCookieTests : 6 1
ePhaseHeaderTests : 2 1

150009 Links Crawled (1)

150009 Links Crawled

archibus.vodacom.co.za:443/fpr/index.as

Finding #	10510220	**Severity**	Information Gathered - Level 1
Unique #	0987569b-652e-49b6-9486-3fb06a2b6285		
Group	Scan Diagnostics		
CWE	-	**Detection Date**	11 Feb 2024 21:02 GMT+0200
OWASP	-		
WASC	-		

Details

Threat

The list of unique links crawled and HTML forms submitted by the scanner appear in the Results section. This list may contain fewer links than the maximum threshold defined.

NOTE: This list also includes:
- All the unique links that are reported in QID 150140 (Redundant links/URL paths crawled and not crawled)
- All the forms reported in QID 150152 (Forms Crawled)
- All the forms in QID 150115 (Authentication Form Found)
- Certain requests from QID 150172 (Requests Crawled)

Impact

N/A

Solution

N/A

Results

Duration of crawl phase (seconds): 1620.00
Number of links: 132

WAS Web Application Report

(This number excludes form requests, ajax links (included in QID 150148) and links re-requested during authentication.)

https://archibus.vodacom.co.za/
https://archibus.vodacom.co.za/FPRWin/
https://archibus.vodacom.co.za/FPRWin/index.aspx
https://archibus.vodacom.co.za/_Incapsula_Resource?CWUDNSAI=23%22xinfo=1-22384977-0%200NNN%20RT%281699815709016%2016037%29%20q%280%20-1%20-1%200%29%20r%280%20-1%29%20B15%284%2c200%2c0%29%20U18%22incident_id=767000500460857534-122447288571202689%22edet=15%22cinfo=04000000%22rpinfo=0%22mth=GET
https://archibus.vodacom.co.za/_Incapsula_Resource?CWUDNSAI=23%22xinfo=11-111956721-0%200NNN%20RT%281694372520954%2015878%29%20q%280%20-1%20-1%200%29%20r%280%20-1%29%20B15%284%2c200%2c0%29%20U18%22incident_id=765000070362200247-5345364212311003 63%22edet=15%22cinfo=04000000%22rpinfo=0%22mth=GET
https://archibus.vodacom.co.za/_Incapsula_Resource?CWUDNSAI=23%22xinfo=11-124742921-0%200NNN%20RT%2816919534170 46%202308%29%20q%280%20-1%20-1%200%29%20r%280%20-1%29%20B15%284%2C200%2C0%29%20U18%22incident_id=128000730324386403-607342817005539915%22edet=15%22cinfo=04000000%22rpinfo=0%22mth=GET
https://archibus.vodacom.co.za/_Incapsula_Resource?CWUDNSAI=23%22xinfo=11-124742921-0%200NNN%20RT%2816919534170 46%202308%29%20q%280%20-1%20-1%200%29%20r%280%20-1%29%20B15%284%2c200%2c0%29%20U18%22incident_id=128000730324386403-607342817005539915%22edet=15%22cinfo=04000000%22rpinfo=0%22mth=GET
https://archibus.vodacom.co.za/_Incapsula_Resource?CWUDNSAI=23%22xinfo=11-140064347-0%200NNN%20RT%2817022349290 44%203123%29%20q%280%20-1%20-1%201%29%20r%280%20-1%29%20B15%284%2C200%2C0%29%20U18%22incident_id=281001070577460321-753234837356747467%22edet=15%22cinfo=04000000%22rpinfo=0%22mth=GET
https://archibus.vodacom.co.za/_Incapsula_Resource?CWUDNSAI=23%22xinfo=11-140064347-0%200NNN%20RT%2817022349290 44%203123%29%20q%280%20-1%20-1%201%29%20r%280%20-1%29%20B15%284%2c200%2c0%29%20U18%22incident_id=281001070577460321-753234837356747467%22edet=15%22cinfo=04000000%22rpinfo=0%22mth=GET
https://archibus.vodacom.co.za/_Incapsula_Resource?CWUDNSAI=23%22xinfo=11-140064348-0%200NNN%20RT%2817022349290 44%2016190%29%20q%280%20-1%20-1%202%29%20r%280%20-1%29%20B15%284%2C200%2C0%29%20U18%22incident_id=281001070577460321-753246536847661771%22edet=15%22cinfo=04000000%22rpinfo=0%22mth=GET
https://archibus.vodacom.co.za/_Incapsula_Resource?CWUDNSAI=23%22xinfo=11-140064348-0%200NNN%20RT%2817022349290 44%2016190%29%20q%280%20-1%20-1%202%29%20r%280%20-1%29%20B15%284%2c200%2c0%29%20U18%22incident_id=281001070577460321-753246536847661771%22edet=15%22cinfo=04000000%22rpinfo=0%22mth=GET
https://archibus.vodacom.co.za/_Incapsula_Resource?CWUDNSAI=23%22xinfo=12-143392341-0%200NNN%20RT%2816919534010 23%20467%29%20q%280%20-1%20-1%201%29%20r%280%20-1%29%20B15%284%2c200%2c0%29%20U18%22incident_id=128000730324386403-688681977104044620%22edet=15%22cinfo=04000000%22rpinfo=0%22mth=GET
https://archibus.vodacom.co.za/_Incapsula_Resource?CWUDNSAI=23%22xinfo=12-182571436-0%200NNN%20RT%2816889294277 53%2015665%29%20q%280%20-1%20-1%202%29%20r%280%20-1%29%20B15%284%2c200%2c0%29%20U18%22incident_id=763001020386100101-868537211589171596%22edet=15%22cinfo=04000000%22rpinfo=0%22mth=GET
https://archibus.vodacom.co.za/_Incapsula_Resource?CWUDNSAI=23%22xinfo=12-77124096-0%200NNN%20RT%2816840909797 06%202875%29%20q%280%20-1%20-1%200%29%20r%280%20-1%29%20B15%284%2c200%2c0%29%20U18%22incident_id=765001090170903434-359187810071944012%22edet=15%22cinfo=04000000%22rpinfo=0%22mth=GET
https://archibus.vodacom.co.za/_Incapsula_Resource?CWUDNSAI=23%22xinfo=12-77127187-0%200NNN%20RT%2816840909958 88%204094%29%20q%280%20-1%20-1%200%29%20r%280%20-1%29%20B15%284%2c200%2c0%29%20U18%22incident_id=765001090170903434-359203417983097676%22edet=15%22cinfo=04000000%22rpinfo=0%22mth=GET
https://archibus.vodacom.co.za/_Incapsula_Resource?CWUDNSAI=23%22xinfo=13-146013152-0%200NNN%20RT%2816999815709015%202793%29%20q%280%20-1%20-1%204%29%20r%280%20-1%29%20B15%284%2c200%2c0%29%20U18%22incident_id=767000500460857534-774752327188810893%22edet=15%22cinfo=04000000%22rpinfo=0%22mth=GET
https://archibus.vodacom.co.za/_Incapsula_Resource?CWUDNSAI=23%22xinfo=13-157825945-0%200NNN%20RT%2816919534215 67%2015799%29%20q%280%20-1%20-1%201%29%20r%280%20-1%29%20B15%284%2c200%2c0%29%20U18%22incident_id=128000730324386403-757535280726020685%22edet=15%22cinfo=04000000%22rpinfo=0%22mth=GET
https://archibus.vodacom.co.za/_Incapsula_Resource?CWUDNSAI=23%22xinfo=13-70594367-0%200NNN%20RT%2816967917929 34%204590%29%20q%280%20-1%20-1%200%29%20r%280%20-1%29%20B15%284%2c200%2c0%29%20U18%22incident_id=766001150280311651-392210022609591501%22edet=15%22cinfo=04000000%22rpinfo=0%22mth=GET
https://archibus.vodacom.co.za/_Incapsula_Resource?CWUDNSAI=23%22xinfo=14-114596260-0%200NNN%20RT%2816865105890 98%204193%29%20q%280%20-1%20-1%203%29%20r%280%20-1%29%20B15%284%2c200%2c0%29%20U18%22incident_id=136700074016808 8542-5478685280383187 34%22edet=15%22cinfo=04000000%22rpinfo=0%22mth=GET
https://archibus.vodacom.co.za/_Incapsula_Resource?CWUDNSAI=23%22xinfo=14-163459825-0%200NNN%20RT%2816943725209 53%202886%29%20q%280%20-1%20-1%200%29%20r%280%20-1%29%20B15%284%2c200%2c0%29%20U18%22incident_id=765000070362200247-772776844095979982%22edet=15%22cinfo=04000000%22rpinfo=0%22mth=GET
https://archibus.vodacom.co.za/_Incapsula_Resource?CWUDNSAI=23%22xinfo=14-98161412-0%200NNN%20RT%2816840909797 10%2016171%29%20q%280%20-1%20-1%200%29%20r%280%20-1%29%20B15%284%2c200%2c0%29%20U18%22incident_id=765001090170903434-451351309958585166%22edet=15%22cinfo=04000000%22rpinfo=0%22mth=GET
https://archibus.vodacom.co.za/_Incapsula_Resource?CWUDNSAI=23%22xinfo=2-16530192-0%200NNN%20RT%2816967917769 89%2015936%29%20q%280%20-1%20-1%200%29%20r%280%20-1%29%20B15%284%2c200%2c0%29%20U18%22incident_id=766001150280311651-854289396771 13538%22edet=15%22cinfo=04000000%22rpinfo=0%22mth=GET
https://archibus.vodacom.co.za/_Incapsula_Resource?CWUDNSAI=23%22xinfo=2-26051945-0%200NNN%20RT%2816943725368 40%204197%29%20q%280%20-1%20-1%200%29%20r%280%20-1%29%20B15%284%2c200%2c0%29%20U18%22incident_id=765000070362200247-129321293534003650%22edet=15%22cinfo=04000000%22rpinfo=0%22mth=GET
https://archibus.vodacom.co.za/_Incapsula_Resource?CWUDNSAI=23%22xinfo=3-53041329-0%200NNN%20RT%2817022349452 42%204178%29%20q%280%20-1%20-1%200%29%20r%280%20-1%29%20B15%284%2c200%2c0%29%20U18%22incident_id=281001070577460321-313704059130944195%22edet=15%22cinfo=04000000%22rpinfo=0%22mth=GET
https://archibus.vodacom.co.za/_Incapsula_Resource?CWUDNSAI=23%22xinfo=32-11389906-0%200NNN%20RT%2817052589717 56%204195%29%20q%280%20-1%20-1%201%29%20r%280%20-1%29%20B15%284%2c200%2c0%29%20U18%22incident_id=168600004022514 2581-6579554901072 3104%22edet=15%22cinfo=04000000%22rpinfo=0%22mth=GET
https://archibus.vodacom.co.za/_Incapsula_Resource?CWUDNSAI=23%22xinfo=5-116739429-0%200NNN%20RT%2816888929427 752%202697%29%20q%280%20-1%20-1%200%29%20r%280%20-1%29%20B15%284%2c200%2c0%29%20U18%22incident_id=763001020386100101-555576851833756037%22edet=15%22cinfo=04000000%22rpinfo=0%22mth=GET
https://archibus.vodacom.co.za/_Incapsula_Resource?CWUDNSAI=23%22xinfo=5-116741115-0%200NNN%20RT%2816888929443 426%204203%29%20q%280%20-1%20-1%200%29%20r%280%20-1%29%20B15%284%2c200%2c0%29%20U18%22incident_id=763001020386100101-555585841200306565%22edet=15%22cinfo=04000000%22rpinfo=0%22mth=GET
https://archibus.vodacom.co.za/_Incapsula_Resource?CWUDNSAI=23%22xinfo=52-10807422-0%200NNN%20RT%2817052589557 14%2016035%29%20q%280%20-1%20-1%201%29%20r%280%20-1%29%20B15%284%2c200%2c0%29%20U18%22incident_id=168600004022514 2581-6184636094178 9492%22edet=15%22cinfo=04000000%22rpinfo=0%22mth=GET
https://archibus.vodacom.co.za/_Incapsula_Resource?CWUDNSAI=23%22xinfo=59-13731742-0%200NNN%20RT%2817052589557 12%202737%29%20q%280%20-1%20-1%201%29%20r%280%20-1%29%20B15%284%2c200%2c0%29%20U18%22incident_id=168600004022514 2581-7866525530442 9883%22edet=15%22cinfo=04000000%22rpinfo=0%22mth=GET
https://archibus.vodacom.co.za/_Incapsula_Resource?CWUDNSAI=23%22xinfo=6-27452916-0%200NNN%20RT%2816865105732 18%202872%29%20q%280%20-1%20-1%200%29%20r%280%20-1%29%20B15%284%2c200%2c0%29%20U18%22incident_id=136700074016808 8542-1420445715471 44838%22edet=15%22cinfo=04000000%22rpinfo=0%22mth=GET
https://archibus.vodacom.co.za/_Incapsula_Resource?CWUDNSAI=23%22xinfo=6-50760056-0%200NNN%20RT%2816919534055 61%209192%29%20q%280%20-1%20-1%200%29%20r%280%20-1%29%20B15%284%2c200%2c0%29%20U18%22incident_id=128000730324386403-257285652188500550%22edet=15%22cinfo=04000000%22rpinfo=0%22mth=GET
https://archibus.vodacom.co.za/_Incapsula_Resource?CWUDNSAI=23%22xinfo=7-38798582-0%200NNN%20RT%2816865105732 18%2015874%29%20q%280%20-1%20-1%200%29%20r%280%20-1%29%20B15%284%2c200%2c0%29%20U18%22incident_id=136700074016808 8542-1993736318053955 91%22edet=15%22cinfo=04000000%22rpinfo=0%22mth=GET
https://archibus.vodacom.co.za/_Incapsula_Resource?CWUDNSAI=23%22xinfo=7-45312743-0%200NNN%20RT%2816967917769 89%202667%29%20q%280%20-1%20-1%200%29%20r%280%20-1%29%20B15%284%2c200%2c0%29%20U18%22incident_id=766001150280311651-263256700448808135%22edet=15%22cinfo=04000000%22rpinfo=0%22mth=GET
https://archibus.vodacom.co.za/_Incapsula_Resource?CWUDNSAI=23%22xinfo=7-68988649-0%200NNN%20RT%2816919534562 71%208%29%20q%280%20-1%20-1%200%29%20r%280%20-1%29%20B15%284%2c200%2c0%29%20U18%22incident_id=128000730324386403-342869859178123847%22edet=15%22cinfo=04000000%22rpinfo=0%22mth=GET
https://archibus.vodacom.co.za/_Incapsula_Resource?CWUDNSAI=23%22xinfo=7-88977006-0%200NNN%20RT%2816998157250 61%204262%29%20q%280%20-1%20-1%202%29%20r%280%20-1%29%20B15%284%2c200%2c0%29%20U18%22incident_id=767000500460857534-474268430816447623%22edet=15%22cinfo=04000000%22rpinfo=0%22mth=GET
https://archibus.vodacom.co.za/_Incapsula_Resource?CWUDNSAI=23&xinfo=1-22384977-0%200NNN%20RT%2816998157090 16%2016037%29%20q%280%20-1%20-1%200%29%20r%280%20-1%29%20B15%284%2C200%2C0%29%20U18&incident_id=767000500460857534-122447288571202689&edet=15&cinfo=04000000&rpinfo=0&mth=GET
https://archibus.vodacom.co.za/_Incapsula_Resource?CWUDNSAI=23&xinfo=1-6094665-0%200NNN%20RT%2817052589653 58%203%29%20q%280%20-1%20-1%200%29%20r%280%20-1%29%20B15%284%2c200%2c0%29%20U18&incident_id=1686000040225142581-367470917550082 57&edet=15&cinfo=04000000&rpinfo=0&mth=GET
https://archibus.vodacom.co.za/_Incapsula_Resource?CWUDNSAI=23&xinfo=10-111982213-0%200NNN%20RT%2816919532991 80%205%29%20q%280%20-1%20-1%20-1%29%20r%280%20-1%29%20B15%284%2c200%2c0%29%20U18&incident_id=128000730324386403-546795125435535946&edet=15&cinfo=04000000&rpinfo=0&mth=GET
https://archibus.vodacom.co.za/_Incapsula_Resource?CWUDNSAI=23&xinfo=10-115212261-0%200NNN%20RT%2816816106689 4793%208%29%20q%280%20-1%20-1%20-1%29%20r%280%20-1%29%20B15%284%2C200%2C0%29%20U18&incident_id=451000960203949962-566675017241401354&edet=15&cinfo=04000000&rpinfo=0&mth=GET
https://archibus.vodacom.co.za/_Incapsula_Resource?CWUDNSAI=23&xinfo=10-115214768-0%200NNN%20RT%2816816106690 9996%203992%29%20q%280%20-1%20-1%200%29%20r%280%20-1%29%20B15%284%2c200%2c0%29%20U18&incident_id=451000960203949962-566690908620396554&edet=15&cinfo=04000000&rpinfo=0&mth=GET
https://archibus.vodacom.co.za/_Incapsula_Resource?CWUDNSAI=23&xinfo=10-126106739-0%200NNN%20RT%2816868929365 204%203%29%20q%280%20-1%20-1%20-1%29%20r%280%20-1%29%20B15%284%2c200%2c0%29%20U18&incident_id=763001020386100101-604542579974543754&edet=15&cinfo=04000000&rpinfo=0&mth=GET
https://archibus.vodacom.co.za/_Incapsula_Resource?CWUDNSAI=23&xinfo=10-129187804-0%200NNN%20RT%2817022349388 29%203%29%20q%280%20-1%20-1%200%29%20r%280%20-1%29%20B15%284%2c200%2c0%29%20U18&incident_id=281001070577460321-698535035818023626&edet=15&cinfo=04000000&rpinfo=0&mth=GET
https://archibus.vodacom.co.za/_Incapsula_Resource?CWUDNSAI=23&xinfo=11-111956721-0%200NNN%20RT%2816943725209 54%2015878%29%20q%280%20-1%20-1%200%29%20r%280%20-1%29%20B15%284%2C200%2C0%29%20U18&incident_id=765000070362200247-534536421231100363&edet=15&cinfo=04000000&rpinfo=0&mth=GET

WAS Web Application Report

https://archibus.vodacom.co.za/_Incapsula_Resource?CWUDNSAI=23&xinfo=11-124742921-0%200NNN%20RT%281691953417046%202308%29%20q%280%20-1%20-1%200%29%20r
%280%20-1%29%20B15%284%2C200%2C0%29%20U18&incident_id=128000730324386403-607342817005539915&edet=15&cinfo=04000000&rpinfo=0&mth=GET
https://archibus.vodacom.co.za/_Incapsula_Resource?CWUDNSAI=23&xinfo=11-140053216-0%200NNN%20RT%281702234866406%206%29%20q%280%20-1%20-1%20-1%29%20r
%280%20-1%29%20B15%284%2c200%2c0%29%20U18&incident_id=281001070577460321-753173814461405899&edet=15&cinfo=04000000&rpinfo=0&mth=GET
https://archibus.vodacom.co.za/_Incapsula_Resource?CWUDNSAI=23&xinfo=11-140064347-0%200NNN%20RT%281702234929044%203123%29%20q%280%20-1%20-1%201%29%20r
%280%20-1%29%20B15%284%2C200%2C0%29%20U18&incident_id=281001070577460321-7532348373567474 67&edet=15&cinfo=04000000&rpinfo=0&mth=GET
https://archibus.vodacom.co.za/_Incapsula_Resource?CWUDNSAI=23&xinfo=11-140064348-0%200NNN%20RT%281702234929044%2016190%29%20q%280%20-1%20-1%202%29%20r
%280%20-1%29%20B15%284%2C200%2C0%29%20U18&incident_id=281001070577460321-7532465368476617 71&edet=15&cinfo=04000000&rpinfo=0&mth=GET
https://archibus.vodacom.co.za/_Incapsula_Resource?CWUDNSAI=23&xinfo=12-133841466-0%200NNN%20RT%281699815698488%205%29%20q%280%20-1%20-1%20-1%29%20r
%280%20-1%29%20B15%284%2c200%2c0%29%20U18&incident_id=76700500460857534-70894421550924097 2&edet=15&cinfo=04000000&rpinfo=0&mth=GET
https://archibus.vodacom.co.za/_Incapsula_Resource?CWUDNSAI=23&xinfo=12-133842840-0%200NNN%20RT%281699815708995%2011%29%20q%280%20-1%20-1%20-1%29%20r
%280%20-1%29%20B15%284%2C200%2C0%29%20U18&incident_id=767000500460857534-708952045234621580&edet=15&cinfo=04000000&rpinfo=0&mth=GET
https://archibus.vodacom.co.za/_Incapsula_Resource?CWUDNSAI=23&xinfo=12-143392341-0%200NNN%20RT%281691953401023%20467%29%20q%280%20-1%20-1%201%29%20r
%280%20-1%29%20B15%284%2C200%2C0%29%20U18&incident_id=128000730324386403-688681977104044620&edet=15&cinfo=04000000&rpinfo=0&mth=GET
https://archibus.vodacom.co.za/_Incapsula_Resource?CWUDNSAI=23&xinfo=12-182571436-0%200NNN%20RT%281688929427753%2015665%29%20q%280%20-1%20-1%202%29%20r
%280%20-1%29%20B15%284%2C200%2C0%29%20U18&incident_id=763001020386100101-868537211589171596&edet=15&cinfo=04000000&rpinfo=0&mth=GET
https://archibus.vodacom.co.za/_Incapsula_Resource?CWUDNSAI=23&xinfo=12-77124096-0%200NNN%20RT%281684090979706%202875%29%20q%280%20-1%20-1%200%29%20r
%280%20-1%29%20B15%284%2C200%2C0%29%20U18&incident_id=765001090170903434-359187810071944012&edet=15&cinfo=04000000&rpinfo=0&mth=GET
https://archibus.vodacom.co.za/_Incapsula_Resource?CWUDNSAI=23&xinfo=12-77127187-0%200NNN%20RT%281684090995888%204094%29%20q%280%20-1%20-1%200%29%20r
%280%20-1%29%20B15%284%2C200%2C0%29%20U18&incident_id=765001090170903434-359203417983097676&edet=15&cinfo=04000000&rpinfo=0&mth=GET
https://archibus.vodacom.co.za/_Incapsula_Resource?CWUDNSAI=23&xinfo=12-95056015-0%200NNN%20RT%281686510510454%2011%29%20q%280%20-1%20-1%20-1%29%20r
%280%20-1%29%20B15%284%2c200%2c0%29%20U18&incident_id=1367000740168088542-463133393133441676&edet=15&cinfo=04000000&rpinfo=0&mth=GET
https://archibus.vodacom.co.za/_Incapsula_Resource?CWUDNSAI=23&xinfo=13-145678257-0%200NNN%20RT%281694372520934%2012%29%20q%280%20-1%20-1%29%20r
%280%20-1%29%20B15%284%2C200%2C0%29%20U18&incident_id=765000070362200247-690227250544312781&edet=15&cinfo=04000000&rpinfo=0&mth=GET
https://archibus.vodacom.co.za/_Incapsula_Resource?CWUDNSAI=23&xinfo=13-146013152-0%200NNN%20RT%281699815709015%202793%29%20q%280%20-1%20-1%204%29%20r
%280%20-1%29%20B15%284%2C200%2C0%29%20U18&incident_id=767000500460857534-774752327188810893&edet=15&cinfo=04000000&rpinfo=0&mth=GET
https://archibus.vodacom.co.za/_Incapsula_Resource?CWUDNSAI=23&xinfo=13-146014798-0%200NNN%20RT%281699815718661%203%29%20q%280%20-1%20-1%200%29%20r
%280%20-1%29%20B15%284%2c200%2c0%29%20U18&incident_id=767000500460857534-774758262833613965&edet=15&cinfo=04000000&rpinfo=0&mth=GET
https://archibus.vodacom.co.za/_Incapsula_Resource?CWUDNSAI=23&xinfo=13-157825945-0%200NNN%20RT%281691953421567%2015799%29%20q%280%20-1%20-1%201%29%20r
%280%20-1%29%20B15%284%2C200%2C0%29%20U18&incident_id=128000730324386403-757535280726020685&edet=15&cinfo=04000000&rpinfo=0&mth=GET
https://archibus.vodacom.co.za/_Incapsula_Resource?CWUDNSAI=23&xinfo=13-165603926-0%200NNN%20RT%281688929427724%2020%29%20q%280%20-1%20-1%20-1%29%20r
%280%20-1%29%20B15%284%2C200%2C0%29%20U18&incident_id=763001020386100101-784253361782987149&edet=15&cinfo=04000000&rpinfo=0&mth=GET
https://archibus.vodacom.co.za/_Incapsula_Resource?CWUDNSAI=23&xinfo=13-70581997-0%200NNN%20RT%2816967917143 11%206%29%20q%280%20-1%20-1%20-1%29%20r
%280%20-1%29%20B15%284%2c200%2c0%29%20U18&incident_id=766001150280311651-392143205803367629&edet=15&cinfo=04000000&rpinfo=0&mth=GET
https://archibus.vodacom.co.za/_Incapsula_Resource?CWUDNSAI=23&xinfo=13-70594367-0%200NNN%20RT%281696791792934%204590%29%20q%280%20-1%20-1%200%29%20r
%280%20-1%29%20B15%284%2C200%2C0%29%20U18&incident_id=766001150280311651-392210022609591501&edet=15&cinfo=04000000&rpinfo=0&mth=GET
https://archibus.vodacom.co.za/_Incapsula_Resource?CWUDNSAI=23&xinfo=13-85261504-0%200NNN%20RT%281684090989049%203%29%20q%280%20-1%20-1%2059%29%20r
%281%20-1%29%20B15%284%2c200%2c0%29%20U18&incident_id=765001090170903434-393561803436399437&edet=15&cinfo=04000000&rpinfo=0&mth=GET
https://archibus.vodacom.co.za/_Incapsula_Resource?CWUDNSAI=23&xinfo=14-114596260-0%200NNN%20RT%281686510589098%204193%29%20q%280%20-1%20-1%203%29%20r
%280%20-1%29%20B15%284%2C200%2C0%29%20U18&incident_id=136700074016808 8542-547868528038318734&edet=15&cinfo=04000000&rpinfo=0&mth=GET
https://archibus.vodacom.co.za/_Incapsula_Resource?CWUDNSAI=23&xinfo=14-163458765-0%200NNN%20RT%281694372517397%203%29%20q%280%20-1%20-1%20-1%29%20r
%281%20-1%29%20B15%284%2c200%2c0%29%20U18&incident_id=765000070362200247-772768924176286158&edet=15&cinfo=04000000&rpinfo=0&mth=GET
https://archibus.vodacom.co.za/_Incapsula_Resource?CWUDNSAI=23&xinfo=14-163459825-0%200NNN%20RT%281694372520953%202886%29%20q%280%20-1%20-1%200%29%20r
%280%20-1%29%20B15%284%2C200%2C0%29%20U18&incident_id=765000070362200247-772776844095979982&edet=15&cinfo=04000000&rpinfo=0&mth=GET
https://archibus.vodacom.co.za/_Incapsula_Resource?CWUDNSAI=23&xinfo=14-98161412-0%200NNN%20RT%281684090979710%2016171%29%20q%280%20-1%20-1%200%29%20r
%280%20-1%29%20B15%284%2C200%2C0%29%20U18&incident_id=765001090170903434-451351309958585166&edet=15&cinfo=04000000&rpinfo=0&mth=GET
https://archibus.vodacom.co.za/_Incapsula_Resource?CWUDNSAI=23&xinfo=2-16530192-0%200NNN%20RT%2816967917776989%2015936%29%20q%280%20-1%20-1%200%29%20r
%280%20-1%29%20B15%284%2C200%2C0%29%20U18&incident_id=766001150280311651-854289396771135 38&edet=15&cinfo=04000000&rpinfo=0&mth=GET
https://archibus.vodacom.co.za/_Incapsula_Resource?CWUDNSAI=23&xinfo=2-26051945-0%200NNN%20RT%281694372536840%204197%29%20q%280%20-1%20-1%200%29%20r
%280%20-1%29%20B15%284%2C200%2C0%29%20U18&incident_id=765000070362200247-129321293534003650&edet=15&cinfo=04000000&rpinfo=0&mth=GET
https://archibus.vodacom.co.za/_Incapsula_Resource?CWUDNSAI=23&xinfo=3-53041329-0%200NNN%20RT%281702234945242%204178%29%20q%280%20-1%20-1%200%29%20r
%280%20-1%29%20B15%284%2C200%2C0%29%20U18&incident_id=281001070577460321-313704059130944195&edet=15&cinfo=04000000&rpinfo=0&mth=GET
https://archibus.vodacom.co.za/_Incapsula_Resource?CWUDNSAI=23&xinfo=31-5366570-0%200NNN%20RT%281705258918883%203%29%20q%280%20-1%20-1%20-1%29%20r
%280%20-1%29%20B15%284%2c200%2c0%29%20U18&incident_id=168600004022514 2581-310325819331054 39&edet=15&cinfo=04000000&rpinfo=0&mth=GET
https://archibus.vodacom.co.za/_Incapsula_Resource?CWUDNSAI=23&xinfo=32-11389906-0%200NNN%20RT%281705258971756%204195%29%20q%280%20-1%20-1%201%29%20r
%280%20-1%29%20B15%284%2C200%2C0%29%20U18&incident_id=168600004022514 2581-657955490107231 04&edet=15&cinfo=04000000&rpinfo=0&mth=GET
https://archibus.vodacom.co.za/_Incapsula_Resource?CWUDNSAI=23&xinfo=37-6911038-0%200NNN%20RT%281705258955691%2015%29%20q%280%20-1%20-1%20-1%29%20r
%280%20-1%29%20B15%284%2C200%2C0%29%20U18&incident_id=168600004022514 2581-405087443719293 81&edet=15&cinfo=04000000&rpinfo=0&mth=GET
https://archibus.vodacom.co.za/_Incapsula_Resource?CWUDNSAI=23&xinfo=4-38615588-0%200NNN%20RT%2816967917865 52%208%29%20q%280%20-1%20-1%200%29%20r
%280%20-1%29%20B15%284%2c200%2c0%29%20U18&incident_id=766001150280311651-201061180251184324&edet=15&cinfo=04000000&rpinfo=0&mth=GET
https://archibus.vodacom.co.za/_Incapsula_Resource?CWUDNSAI=23&xinfo=5-109279300-0%200NNN%20RT%281681066903598%208%29%20q%280%20-1%20-1%201%29%20r
%280%20-1%29%20B15%284%2c200%2c0%29%20U18&incident_id=451000960203949962-528949510572021765&edet=15&cinfo=04000000&rpinfo=0&mth=GET
https://archibus.vodacom.co.za/_Incapsula_Resource?CWUDNSAI=23&xinfo=5-116739429-0%200NNN%20RT%281688929427752%202697%29%20q%280%20-1%20-1%200%29%20r
%280%20-1%29%20B15%284%2C200%2C0%29%20U18&incident_id=763001020386100101-555576851833756037&edet=15&cinfo=04000000&rpinfo=0&mth=GET
https://archibus.vodacom.co.za/_Incapsula_Resource?CWUDNSAI=23&xinfo=5-116740391-0%200NNN%20RT%281688929436725%203%29%20q%280%20-1%20-1%200%29%20r
%280%20-1%29%20B15%284%2c200%2c0%29%20U18&incident_id=763001020386100101-555579935620274565&edet=15&cinfo=04000000&rpinfo=0&mth=GET
https://archibus.vodacom.co.za/_Incapsula_Resource?CWUDNSAI=23&xinfo=5-116741115-0%200NNN%20RT%281688929443426%204203%29%20q%280%20-1%20-1%200%29%20r
%280%20-1%29%20B15%284%2C200%2C0%29%20U18&incident_id=763001020386100101-555585841200306565&edet=15&cinfo=04000000&rpinfo=0&mth=GET
https://archibus.vodacom.co.za/_Incapsula_Resource?CWUDNSAI=23&xinfo=52-10807422-0%200NNN%20RT%281705258955714%2016035%29%20q%280%20-1%20-1%201%29%20r
%280%20-1%29%20B15%284%2C200%2C0%29%20U18&incident_id=168600004022514 2581-618463609417894 92&edet=15&cinfo=04000000&rpinfo=0&mth=GET
https://archibus.vodacom.co.za/_Incapsula_Resource?CWUDNSAI=23&xinfo=59-13731742-0%200NNN%20RT%281705258955712%202737%29%20q%280%20-1%20-1%201%29%20r
%280%20-1%29%20B15%284%2C200%2C0%29%20U18&incident_id=168600004022514 2581-786652553044298 83&edet=15&cinfo=04000000&rpinfo=0&mth=GET
https://archibus.vodacom.co.za/_Incapsula_Resource?CWUDNSAI=23&xinfo=6-27452916-0%200NNN%20RT%281686510573218%202872%29%20q%280%20-1%20-1%200%29%20r
%280%20-1%29%20B15%284%2C200%2C0%29%20U18&incident_id=136700074016808 8542-142044571547144838&edet=15&cinfo=04000000&rpinfo=0&mth=GET
https://archibus.vodacom.co.za/_Incapsula_Resource?CWUDNSAI=23&xinfo=6-50760056-0%200NNN%20RT%281691953405561%209192%29%20q%280%20-1%20-1%200%29%20r
%280%20-1%29%20B15%284%2C200%2C0%29%20U18&incident_id=128000730324386403-257285652188500550&edet=15&cinfo=04000000&rpinfo=0&mth=GET
https://archibus.vodacom.co.za/_Incapsula_Resource?CWUDNSAI=23&xinfo=6-87530002-0%200NNN%20RT%281702234929023%2013%29%20q%280%20-1%20-1%20-1%29%20r
%280%20-1%29%20B15%284%2C200%2C0%29%20U18&incident_id=281001070577460321-492085024575265478&edet=15&cinfo=04000000&rpinfo=0&mth=GET
https://archibus.vodacom.co.za/_Incapsula_Resource?CWUDNSAI=23&xinfo=7-38318934-0%200NNN%20RT%281684090979688%2011%29%20q%280%20-1%20-1%20-1%29%20r
%280%20-1%29%20B15%284%2C200%2C0%29%20U18&incident_id=765001090170903434-178457729444944711&edet=15&cinfo=04000000&rpinfo=0&mth=GET
https://archibus.vodacom.co.za/_Incapsula_Resource?CWUDNSAI=23&xinfo=7-38798582-0%200NNN%20RT%281686510573218%2015874%29%20q%280%20-1%20-1%200%29%20r
%280%20-1%29%20B15%284%2C200%2C0%29%20U18&incident_id=136700074016808 8542-199373631805395591&edet=15&cinfo=04000000&rpinfo=0&mth=GET
https://archibus.vodacom.co.za/_Incapsula_Resource?CWUDNSAI=23&xinfo=7-45312741-0%200NNN%20RT%2816967917769 69%2011%29%20q%280%20-1%20-1%20-1%29%20r
%280%20-1%29%20B15%284%2C200%2C0%29%20U18&incident_id=766001150280311651-263255351829077191&edet=15&cinfo=04000000&rpinfo=0&mth=GET
https://archibus.vodacom.co.za/_Incapsula_Resource?CWUDNSAI=23&xinfo=7-45312743-0%200NNN%20RT%2816967917769 89%202667%29%20q%280%20-1%20-1%200%29%20r

%280%20-1%29%20B15%284%2C200%2C0%29%20U18&incident_id=766001150280311651-263256700448808135&edet=15&cinfo=04000000&rpinfo=0&mth=GET
https://archibus.vodacom.co.za/_Incapsula_Resource?CWUDNSAI=23&xinfo=7-68982489-0%200NNN%20RT%2816919534079 64%203%29%20q%280%20-1%20-1%200%29%20r
%280%20-1%29%20B15%284%2c200%2c0%29%20U18&incident_id=12800073032438 6403-342838544571568711&edet=15&cinfo=04000000&rpinfo=0&mth=GET
https://archibus.vodacom.co.za/_Incapsula_Resource?CWUDNSAI=23&xinfo=7-77442269-0%200NNN%20RT%2816943725301 58%203%29%20q%280%20-1%20-1%201%29%20r
%280%20-1%29%20B15%284%2c200%2c0%29%20U18&incident_id=765000070362200247-368447231281136071&edet=15&cinfo=04000000&rpinfo=0&mth=GET
https://archibus.vodacom.co.za/_Incapsula_Resource?CWUDNSAI=23&xinfo=7-88977006-0%200NNN%20RT%2816998157250 61%204262%29%20q%280%20-1%20-1%202%29%20r
%280%20-1%29%20B15%284%2C200%2C0%29%20U18&incident_id=767000500460857534-474268430816447623&edet=15&cinfo=04000000&rpinfo=0&mth=GET
https://archibus.vodacom.co.za/_Incapsula_Resource?CWUDNSAI=23&xinfo=8-33065898-0%200NNN%20RT%2816840909760 99%204%29%20q%280%20-1%20-1%20-1%29%20r
%280%20-1%29%20B15%284%2c200%2c0%29%20U18&incident_id=765001090170903434-155918222111873864&edet=15&cinfo=04000000&rpinfo=0&mth=GET
https://archibus.vodacom.co.za/_Incapsula_Resource?CWUDNSAI=23&xinfo=8-63631571-0%200NNN%20RT%2816810668741 98%203%29%20q%280%20-1%20-1%20-1%29%20r
%280%20-1%29%20B15%284%2c200%2c0%29%20U18&incident_id=451000960203949962-322508943962347528&edet=15&cinfo=04000000&rpinfo=0&mth=GET
https://archibus.vodacom.co.za/_Incapsula_Resource?CWUDNSAI=23&xinfo=8-63633300-0%200NNN%20RT%2816810668948 08%202364%29%20q%280%20-1%20-1%200%29%20r
%280%20-1%29%20B15%284%2C200%2C0%29%20U18&incident_id=451000960203949962-322517894674192392&edet=15&cinfo=04000000&rpinfo=0&mth=GET
https://archibus.vodacom.co.za/_Incapsula_Resource?CWUDNSAI=23&xinfo=8-63633300-0%200NNN%20RT%2816810668948 08%202364%29%20q%280%20-1%20-1%200%29%20r
%280%20-1%29%20B15%284%2c200%2c0%29%20U18&incident_id=451000960203949962-322517894674192392&edet=15&cinfo=04000000&rpinfo=0&mth=GET
https://archibus.vodacom.co.za/_Incapsula_Resource?CWUDNSAI=23&xinfo=8-71774864-0%200NNN%20RT%2816919533986 94%2013%29%20q%280%20-1%20-1%20-1%29%20r
%280%20-1%29%20B15%284%2C200%2C0%29%20U18&incident_id=128000730324386403-355338754828800584&edet=15&cinfo=04000000&rpinfo=0&mth=GET
https://archibus.vodacom.co.za/_Incapsula_Resource?CWUDNSAI=23&xinfo=9-55870156-0%200NNN%20RT%2816865105732 00%209%29%20q%280%20-1%20-1%20-1%29%20r
%280%20-1%29%20B15%284%2C200%2C0%29%20U18&incident_id=136700074016808 8542-281155358218982025&edet=15&cinfo=04000000&rpinfo=0&mth=GET
https://archibus.vodacom.co.za/_Incapsula_Resource?CWUDNSAI=23&xinfo=9-55871876-0%200NNN%20RT%2816865105824 39%205%29%20q%280%20-1%20-1%201%29%20r
%280%20-1%29%20B15%284%2c200%2c0%29%20U18&incident_id=136700074016808 8542-281164046937821833&edet=15&cinfo=04000000&rpinfo=0&mth=GET
https://archibus.vodacom.co.za/_Incapsula_Resource?CWUDNSAI=23&xinfo=9-89541750-0%200NNN%20RT%2816810668948 09%2015180%29%20q%280%20-1%20-1%200%29%20r
%280%20-1%29%20B15%284%2C200%2C0%29%20U18&incident_id=451000960203949962-436656818069116937&edet=15&cinfo=04000000&rpinfo=0&mth=GET
https://archibus.vodacom.co.za/_Incapsula_Resource?CWUDNSAI=23&xinfo=9-89541750-0%200NNN%20RT%2816810668948 09%2015180%29%20q%280%20-1%20-1%200%29%20r
%280%20-1%29%20B15%284%2c200%2c0%29%20U18&incident_id=451000960203949962-436656818069116937&edet=15&cinfo=04000000&rpinfo=0&mth=GET
https://archibus.vodacom.co.za/_Incapsula_Resource?SWKMTFSR=1&e=0.11641625286643564
https://archibus.vodacom.co.za/_Incapsula_Resource?SWKMTFSR=1&e=0.12523218982415463
https://archibus.vodacom.co.za/_Incapsula_Resource?SWKMTFSR=1&e=0.1518548352222595
https://archibus.vodacom.co.za/_Incapsula_Resource?SWKMTFSR=1&e=0.2643588357059361
https://archibus.vodacom.co.za/_Incapsula_Resource?SWKMTFSR=1&e=0.39046879017373204
https://archibus.vodacom.co.za/_Incapsula_Resource?SWKMTFSR=1&e=0.7202531631723876
https://archibus.vodacom.co.za/_Incapsula_Resource?SWKMTFSR=1&e=0.7769744014860993
https://archibus.vodacom.co.za/_Incapsula_Resource?SWKMTFSR=1&e=0.951256226805095
https://archibus.vodacom.co.za/csp_report
https://archibus.vodacom.co.za/docs/
https://archibus.vodacom.co.za/docs/RELEASE-NOTES.txt
https://archibus.vodacom.co.za/docs/api/
https://archibus.vodacom.co.za/docs/api/index.html
https://archibus.vodacom.co.za/docs/appdev/
https://archibus.vodacom.co.za/docs/changelog.html
https://archibus.vodacom.co.za/docs/cluster-howto.html
https://archibus.vodacom.co.za/docs/config/
https://archibus.vodacom.co.za/docs/deployer-howto.html
https://archibus.vodacom.co.za/docs/jndi-datasource-examples-howto.html
https://archibus.vodacom.co.za/docs/manager-howto.html
https://archibus.vodacom.co.za/docs/realm-howto.html
https://archibus.vodacom.co.za/docs/security-howto.html
https://archibus.vodacom.co.za/docs/setup.html
https://archibus.vodacom.co.za/examples/
https://archibus.vodacom.co.za/favicon.ico
https://archibus.vodacom.co.za/fpr/
https://archibus.vodacom.co.za/fpr/index.asp
https://archibus.vodacom.co.za/fpr/null
https://archibus.vodacom.co.za/host-manager/
https://archibus.vodacom.co.za/host-manager/html
https://archibus.vodacom.co.za/manager/
https://archibus.vodacom.co.za/manager/html
https://archibus.vodacom.co.za/manager/status
https://archibus.vodacom.co.za/null

150010 External Links Discovered (1)

150010 External Links Discovered

archibus.vodacom.co.za:443/fpr/index.as

Finding #	10510217	**Severity**	Information Gathered - Level 1
Unique #	ad2e450c-b785-4dd3-aa05-937a153bba6b		
Group	Scan Diagnostics		
CWE	-	**Detection Date**	11 Feb 2024 21:02 GMT+0200
OWASP	-		
WASC	-		

Details

Threat

External links discovered during the scan are listed in the Results section. These links were out of scope for the scan and were not crawled.

Impact
N/A

Solution
N/A

Results

Number of links: 32
https://www.imperva.com/why-am-i-seeing-this-page/?src=23%22utm_source=blockingpages
https://www.imperva.com/why-am-i-seeing-this-page/?src=23&utm_source=blockingpages
https://github.com/apache/tomcat/tree/9.0.x
https://fonts.gstatic.com/s/inter/v13/UcC73FwrK3iLTeHuS_fvQtMwCp50KnMa1ZL7.woff2
https://fonts.googleapis.com/css2?family=Inter:wght@300;400;500;700%22display=swap
https://fonts.googleapis.com/css2?family=Inter:wght@300;400;500;700&display=swap
https://wiki.apache.org/tomcat/FrontPage
https://wiki.apache.org/tomcat/Specifications
https://wiki.apache.org/tomcat/TomcatVersions
https://tomcat.apache.org/
https://tomcat.apache.org/bugreport.html
https://tomcat.apache.org/connectors-doc/
https://tomcat.apache.org/contact.html
https://tomcat.apache.org/download-connectors.cgi
https://tomcat.apache.org/download-native.cgi
https://tomcat.apache.org/faq/
https://tomcat.apache.org/findhelp.html
https://tomcat.apache.org/getinvolved.html
https://tomcat.apache.org/heritage.html
https://tomcat.apache.org/legal.html
https://tomcat.apache.org/lists.html
https://tomcat.apache.org/migration.html
https://tomcat.apache.org/native-doc/
https://tomcat.apache.org/resources.html
https://tomcat.apache.org/security.html
https://tomcat.apache.org/source.html
https://tomcat.apache.org/taglibs/
https://tomcat.apache.org/whoweare.html
https://www.apache.org/
https://www.apache.org/foundation/sponsorship.html
https://www.apache.org/foundation/thanks.html
http://go.microsoft.com/fwlink/?linkid=66138%22clcid%3D0x409

150020 Links Rejected By Crawl Scope or Exclusion List (1)

150020 Links Rejected By Crawl Scope or Exclusion List

archibus.vodacom.co.za:443/fpr/index.as

Finding #	10510004	**Severity**	Information Gathered - Level 1
Unique #	940db9e6-1f7e-4c36-83be-570d1fb6468f		
Group	Scan Diagnostics		
CWE	-	**Detection Date**	11 Feb 2024 21:02 GMT+0200
OWASP	-		
WASC	-		

Details

Threat
One or more links were not crawled because of an explicit rule to exclude them. This also occurs if a link is malformed.

Exclude list and Include list entries can cause links to be rejected. If a scan is limited to a specific starting directory, then links outside that directory will neither be crawled or tested.

Links that contain a host name or IP address different from the target application are considered external links and not crawled by default; those types of links are not listed here. This often happens when the scope of a scan is limited to the directory of the starting URL. The scope can be changed in the Web

WAS Web Application Report

Application Record.

During the test phase, some path-based tests may be rejected if the scan is limited to the directory of the starting URL and the test would fall outside that directory. In these cases, the number of rejected links may be too high to list in the Results section.

Impact
Links listed here were neither crawled or tested by the Web application scanning engine.

Solution
A link might have been intentionally matched by a exclude or include list entry. Verify that no links in this list were unintentionally rejected.

Results

Links not permitted:
(This list includes links from QIDs: 150010,150041,150143,150170)

External links discovered:
https://www.imperva.com/why-am-i-seeing-this-page/?src=23%22utm_source=blockingpages
https://www.imperva.com/why-am-i-seeing-this-page/?src=23&utm_source=blockingpages
https://github.com/apache/tomcat/tree/9.0.x
https://fonts.gstatic.com/s/inter/v13/UcC73FwrK3iLTeHuS_fvQtMwCp50KnMa1ZL7.woff2
https://fonts.googleapis.com/css2?family=Inter:wght@300;400;500;700%22display=swap
https://fonts.googleapis.com/css2?family=Inter:wght@300;400;500;700&display=swap
https://wiki.apache.org/tomcat/FrontPage
https://wiki.apache.org/tomcat/Specifications
https://wiki.apache.org/tomcat/TomcatVersions
https://tomcat.apache.org/

IP based excluded links:
Links rejected during the test phase not reported due to volume of links.

150021 Scan Diagnostics (1)

150021 Scan Diagnostics

archibus.vodacom.co.za:443/fpr/index.as

Finding #	10510205	**Severity**	Information Gathered - Level 1
Unique #	59351b3c-719f-4dae-90fb-bef9372f5e34		
Group	Scan Diagnostics		
CWE	-	**Detection Date**	11 Feb 2024 21:02 GMT+0200
OWASP	-		
WASC	-		

Details

Threat
This check provides various details of the scan's performance and behavior. In some cases, this check can be used to identify problems that the scanner encountered when crawling the target Web application.

Impact
The scan diagnostics data provides technical details about the crawler's performance and behavior. This information does not necessarily imply problems with the Web application.

Solution
No action is required.

Results

Loaded 4 exclude list entries.
Loaded 0 allow list entries.

WAS Web Application Report

HTML form authentication unavailable, no WEBAPP entry found
Target web application page https://archibus.vodacom.co.za/fpr/index.asp fetched. Status code:404, Content-Type:text/html, load time:1 milliseconds.
Batch #0 VirtualHostDiscovery: estimated time < 10 minutes (70 tests, 0 inputs)
VirtualHostDiscovery: 70 vulnsigs tests, completed 70 requests, 829 seconds. Completed 70 requests of 70 estimated requests (100%). All tests completed.
Batch #0 SameSiteScripting: estimated time < 1 minute (2 tests, 0 inputs)
SameSiteScripting: 2 vulnsigs tests, completed 2 requests, 0 seconds. Completed 2 requests of 2 estimated requests (100%). All tests completed.
Batch #0 CMSDetection: estimated time < 10 minutes (1 tests, 1 inputs)
[CMSDetection phase] : No potential CMS found using Blind Elephant algorithm. Aborting the CMS Detection phase
CMSDetection: 1 vulnsigs tests, completed 56 requests, 26 seconds. Completed 56 requests of 56 estimated requests (100%). All tests completed.
No more requeues, redundant link threshold has been surpassed.
Collected 163 links overall in 0 hours 27 minutes duration.
Batch #0 BannersVersionReporting: estimated time < 1 minute (1 tests, 1 inputs)
BannersVersionReporting: 1 vulnsigs tests, completed 0 requests, 0 seconds. Completed 0 requests of 1 estimated requests (0%). All tests completed.
Path manipulation: Estimated requests (payloads x links): files with extension:(0 x 13) + files:(0 x 122) + directories:(9 x 10) + paths:(0 x 132) = total (90)
Batch #0 WS Directory Path manipulation: estimated time < 1 minute (9 tests, 132 inputs)
WS Directory Path manipulation: 9 vulnsigs tests, completed 90 requests, 63 seconds. Completed 90 requests of 90 estimated requests (100%). All tests completed.
Batch #0 WS enumeration: estimated time < 10 minutes (11 tests, 132 inputs)
WS enumeration: 11 vulnsigs tests, completed 26 requests, 300 seconds. Completed 26 requests of 1452 estimated requests (1.79063%). Some tests were skipped due to errors.
Batch #1 URI parameter manipulation (no auth): estimated time < 10 minutes (125 tests, 9 inputs)
Batch #1 URI parameter manipulation (no auth): 125 vulnsigs tests, completed 1089 requests, 265 seconds. Completed 1089 requests of 1125 estimated requests (96.8%). Some tests were skipped due to errors.
Batch #1 URI parameter name manipulation (no auth): estimated time < 10 minutes (125 tests, 9 inputs)
Batch #1 URI parameter name manipulation (no auth): 125 vulnsigs tests, completed 246 requests, 1 seconds. Completed 246 requests of 1125 estimated requests (21.8667%). All tests completed.
Batch #1 URI blind SQL manipulation (no auth): estimated time < 1 minute (13 tests, 9 inputs)
Batch #1 URI blind SQL manipulation (no auth): 13 vulnsigs tests, completed 288 requests, 0 seconds. Completed 288 requests of 351 estimated requests (82.0513%). All tests completed.
Batch #1 URI parameter time-based tests (no auth): estimated time < 1 minute (19 tests, 9 inputs)
Batch #1 URI parameter time-based tests (no auth): 19 vulnsigs tests, completed 171 requests, 0 seconds. Completed 171 requests of 171 estimated requests (100%). All tests completed.
Batch #1 URI parameter time-based tests for Apache Struts Vulnerabilities (no auth): estimated time < 1 minute (1 tests, 9 inputs)
Batch #1 URI parameter time-based tests for Apache Struts Vulnerabilities (no auth): 1 vulnsigs tests, completed 9 requests, 0 seconds. Completed 9 requests of 9 estimated requests (100%). All tests completed.
Batch #4 WebCgiOob: estimated time < 30 minutes (133 tests, 1 inputs)
Batch #4 WebCgiOob: 133 vulnsigs tests, completed 192 requests, 401 seconds. Completed 192 requests of 20460 estimated requests (0.938416%). All tests completed.
No XML requests found. Skipping XXE tests.
Batch #4 DOM XSS exploitation: estimated time < 1 minute (4 tests, 0 inputs)
Batch #4 DOM XSS exploitation: 4 vulnsigs tests, completed 0 requests, 1 seconds. No tests to execute.
Batch #4 HTTP call manipulation: estimated time < 1 minute (59 tests, 0 inputs)
Batch #4 HTTP call manipulation: 59 vulnsigs tests, completed 0 requests, 0 seconds. No tests to execute.
Batch #4 Open Redirect analysis: estimated time < 1 minute (2 tests, 1 inputs)
Batch #4 Open Redirect analysis: 2 vulnsigs tests, completed 2 requests, 12 seconds. Completed 2 requests of 2 estimated requests (100%). All tests completed.
CSRF tests will not be launched because the scan is not successfully authenticated.
Batch #4 File Inclusion analysis: estimated time < 1 minute (1 tests, 134 inputs)
Batch #4 File Inclusion analysis: 1 vulnsigs tests, completed 0 requests, 0 seconds. Completed 0 requests of 134 estimated requests (0%). All tests completed.
Batch #4 Cookie manipulation: estimated time < 10 minutes (76 tests, 4 inputs)
Batch #4 Cookie manipulation: 76 vulnsigs tests, completed 6431 requests, 495 seconds. Completed 6431 requests of 6344 estimated requests (101.371%). XSS optimization removed 3050 links. All tests completed.
Batch #4 Header manipulation: estimated time < 30 minutes (76 tests, 61 inputs)
Batch #4 Header manipulation: 76 vulnsigs tests, completed 11329 requests, 535 seconds. Completed 11329 requests of 24888 estimated requests (45.5199%). XSS optimization removed 3050 links. All tests completed.
Batch #4 shell shock detector: estimated time < 1 minute (1 tests, 61 inputs)
Batch #4 shell shock detector: 1 vulnsigs tests, completed 61 requests, 0 seconds. Completed 61 requests of 61 estimated requests (100%). All tests completed.
Batch #4 shell shock detector(form): estimated time < 1 minute (1 tests, 0 inputs)
Batch #4 shell shock detector(form): 1 vulnsigs tests, completed 0 requests, 0 seconds. No tests to execute.
Login Brute Force manipulation estimated time: no tests enabled
Login Brute Force manipulation estimated time: no tests enabled
Batch #5 HTTP Time Bandit: estimated time < 1 minute (1 tests, 10 inputs)
Batch #5 HTTP Time Bandit: 1 vulnsigs tests, completed 200 requests, 7 seconds. No tests to execute.
Path manipulation: Estimated requests (payloads x links): files with extension:(1 x 13) + files:(0 x 122) + directories:(4 x 10) + paths:(14 x 132) = total (1901)
Batch #5 Path XSS manipulation: estimated time < 10 minutes (19 tests, 132 inputs)
Batch #5 Path XSS manipulation: 19 vulnsigs tests, completed 489 requests, 1 seconds. Completed 489 requests of 1901 estimated requests (25.7233%). All tests completed.
Path manipulation: Estimated requests (payloads x links): files with extension:(0 x 13) + files:(0 x 122) + directories:(1 x 10) + paths:(0 x 132) = total (10)
Batch #5 Tomcat Vuln manipulation: estimated time < 1 minute (1 tests, 132 inputs)
Batch #5 Tomcat Vuln manipulation: 1 vulnsigs tests, completed 9 requests, 0 seconds. Completed 9 requests of 10 estimated requests (90%). All tests completed.
Path manipulation: Estimated requests (payloads x links): files with extension:(0 x 13) + files:(0 x 122) + directories:(16 x 10) + paths:(0 x 132) = total (160)
Batch #5 Time based path manipulation: estimated time < 1 minute (16 tests, 134 inputs)
Batch #5 Time based path manipulation: 16 vulnsigs tests, completed 96 requests, 0 seconds. Completed 96 requests of 160 estimated requests (60%). All tests completed.
Path manipulation: Estimated requests (payloads x links): files with extension:(4 x 13) + files:(18 x 122) + directories:(152 x 10) + paths:(19 x 132) = total (6276)
Batch #5 Path manipulation: estimated time < 10 minutes (193 tests, 132 inputs)
Batch #5 Path manipulation: 193 vulnsigs tests, completed 2062 requests, 153 seconds. Completed 2062 requests of 6276 estimated requests (32.8553%). All tests completed.
Batch #5 WebCgiHrs: estimated time < 1 minute (1 tests, 1 inputs)
Batch #5 WebCgiHrs: 1 vulnsigs tests, completed 6 requests, 0 seconds. Completed 6 requests of 264 estimated requests (2.27273%). All tests completed.
Batch #5 WebCgiGeneric: estimated time < 1 hours (451 tests, 1 inputs)
Batch #5 WebCgiGeneric: 451 vulnsigs tests, completed 9566 requests, 776 seconds. Completed 9566 requests of 79860 estimated requests (11.9785%). All tests completed.
Batch #5 Open Redirect analysis: estimated time < 1 minute (2 tests, 1 inputs)
Batch #5 Open Redirect analysis: 2 vulnsigs tests, completed 0 requests, 5 seconds. Completed 0 requests of 2 estimated requests (0%). All tests completed.
Duration of Crawl Time: 1620.00 (seconds)
Duration of Test Phase: 3719.00 (seconds)
Total Scan Time: 5339.00 (seconds)

Total requests made: 33648
Average server response time: 0.19 seconds

Average browser load time: 0.19 seconds

WAS Web Application Report

150028 Cookies Collected (1)

150028 Cookies Collected

archibus.vodacom.co.za:443/fpr/index.as

Finding #	10510210	**Severity**	Information Gathered - Level 1
Unique #	aaf57a3f-c7cb-40d2-b3d6-46bd3e12c714		
Group	Scan Diagnostics		
CWE	-	**Detection Date**	11 Feb 2024 21:02 GMT+0200
OWASP	-		
WASC	-		

Details

Threat

The cookies listed in the Results section were set by the web application during the crawl phase.

Impact

Cookies may potentially contain sensitive information about the user.

Note: Long scan duration can occur if a web application sets a large number of cookies (e.g., 25 cookies or more) and QIDs 150002, 150046, 150047, and 150048 are enabled.

Solution

Review cookie values to ensure they do not include sensitive information. If scan duration is excessive due to a large number of cookies, consider excluding QIDs 150002, 150046, 150047, and 150048.

Results

Total cookies: 4
visid_incap_2776849=XzGtDabQTHuVkbHOgCNGXPUZyWUAAAAAQUIPAAAAAABzHTfqgLA/hAMNNToBRAEF; HttpOnly; expires=Sun, 09-Feb-2025 22:21:08 GMT; domain=.vodacom.co.za; path=/ First set at URL: https://archibus.vodacom.co.za/fpr/index.asp
nlbi_2776849=1uvTSns0kGzwA8rXZU49BAAAAABumPnVc6r7kZo+kAK6WiUr; domain=.vodacom.co.za; path=/ First set at URL: https://archibus.vodacom.co.za/fpr/index.asp
incap_ses_1687_2776849=ArRnARTRdWEO7PgfvG1pF/UZyWUAAAAACho9ich3SZo+8LGHMtIyTQ==; domain=.vodacom.co.za; path=/ First set at URL: https://archibus.vodacom.co.za/fpr/index.asp
nlbi_2776849_2147483392=a6JeKHL+xgNWhQdiZU49BAAAAABtrQ53JjbMXz9smE8uFxJx; domain=.vodacom.co.za; path=/ First set at URL: https://archibus.vodacom.co.za/fpr/index.asp

150097 HTTP Response Indicates Scan May Be Blocked (1)

150097 HTTP Response Indicates Scan May Be Blocked

archibus.vodacom.co.za:443/fpr/index.as

Finding #	10510213	**Severity**	Information Gathered - Level 1
Unique #	7eeabcfb-fa84-4808-9890-5b3aad8efa6e		
Group	Scan Diagnostics		
CWE	-	**Detection Date**	11 Feb 2024 21:02 GMT+0200
OWASP	-		
WASC	-		

Details

Threat

The scanner received an HTTP response from the target web site that contains a message indicating the scan has been blocked. This often occurs due to an intermediate security device such as a web application firewall (WAF), intrusion detection system (IDS), or intrusion prevention system (IPS).

Impact

If the scanner's IP or traffic has been blocked, then the results of the scan will be empty or incomplete because the web site could not be successfully crawled and tested.

Solution

Modify relevant security rules so that the WAS scans will not trigger alerts or be otherwise blocked. Additionally, review 150528 for additional HTTP 4XX Error Code responses found during the scanning.

Results

Uri: https://archibus.vodacom.co.za/_Incapsula_Resource?CWUDNSAI=23&xinfo=1-22384977-0%200NNN%20RT%281699815709016%2016037%29%20q%280%20-1%20-1%200%29%20r%280%20-1%29%20B15%284%2C200%2C0%29%20U18&incident_id=767000500460857534-122447288571202689&edet=15&cinfo=04000000&rpinfo=0&mth=GET
Match: pan>

Powered by
Imperva

</body></html>

Uri: https://archibus.vodacom.co.za/_Incapsula_Resource?CWUDNSAI=23&xinfo=1-6094665-0%200NNN%20RT%281705258965358%203%29%20q%280%20-1%20-1%200%29%20r%280%20-1%29%20B15%284%2c200%2c0%29%20U18&incident_id=1686000040225142581-36747091755008257&edet=15&cinfo=04000000&rpinfo=0&mth=GET
Match: pan>

Powered by
Imperva

</body></html>

Uri: https://archibus.vodacom.co.za/_Incapsula_Resource?CWUDNSAI=23&xinfo=10-111982213-0%200NNN%20RT%281691953299180%205%29%20q%280%20-1%20-1%20-1%29%20r%280%20-1%29%20B15%284%2c200%2c0%29%20U18&incident_id=128000730324386403-546795125435535946&edet=15&cinfo=04000000&rpinfo=0&mth=GET
Match: pan>

Powered by
Imperva

</body></html>

Uri: https://archibus.vodacom.co.za/_Incapsula_Resource?CWUDNSAI=23&xinfo=10-115212261-0%200NNN%20RT%281681066894793%208%29%20q%280%20-1%20-1%20-1%29%20r%280%20-1%29%20B15%284%2C200%2C0%29%20U18&incident_id=451000960203949962-566675017241401354&edet=15&cinfo=04000000&rpinfo=0&mth=GET
Match: pan>

Powered by
Imperva

</body></html>

Uri: https://archibus.vodacom.co.za/_Incapsula_Resource?CWUDNSAI=23&xinfo=10-126106739-0%200NNN%20RT%281688929365204%203%29%20q%280%20-1%20-1%20-1%29%20r%280%20-1%29%20B15%284%2c200%2c0%29%20U18&incident_id=763001020386100101-604542579974543754&edet=15&cinfo=04000000&rpinfo=0&mth=GET
Match: pan>

Powered by
Imperva

</body></html>

Uri: https://archibus.vodacom.co.za/_Incapsula_Resource?CWUDNSAI=23&xinfo=10-115214768-0%200NNN%20RT%281681066909996%203992%29%20q%280%20-1%20-1%200%29%20r%280%20-1%29%20B15%284%2c200%2c0%29%20U18&incident_id=451000960203949962-566690908620396554&edet=15&cinfo=04000000&rpinfo=0&mth=GET
Match: pan>

Powered by
Imperva

</body></html>

Uri: https://archibus.vodacom.co.za/_Incapsula_Resource?CWUDNSAI=23&xinfo=10-129187804-0%200NNN%20RT%2817022349388 29%203%29%20q%280%20-1%20-1%200%29%20r%280%20-1%29%20B15%284%2c200%2c0%29%20U18&incident_id=281001070577460321-698535035818023626&edet=15&cinfo=04000000&rpinfo=0&mth=GET
Match: pan>

Powered by
Imperva

</body></html>

Uri: https://archibus.vodacom.co.za/_Incapsula_Resource?CWUDNSAI=23&xinfo=11-111956721-0%200NNN%20RT%2816943725209 54%2015878%29%20q%280%20-1%20-1%200%29%20r%280%20-1%29%20B15%284%2C200%2C0%29%20U18&incident_id=765000070362200247-534536421231100363&edet=15&cinfo=04000000&rpinfo=0&mth=GET
Match: pan>

Powered by
Imperva

</body></html>

Uri: https://archibus.vodacom.co.za/_Incapsula_Resource?CWUDNSAI=23&xinfo=52-10807422-0%200NNN%20RT%2817052589557 14%2016035%29%20q%280%20-1%20-1%201%29%20r%280%20-1%29%20B15%284%2C200%2C0%29%20U18&incident_id=168600004022514258 1-61846360941789492&edet=15&cinfo=04000000&rpinfo=0&mth=GET
Match: pan>

Powered by
Imperva

</body></html>

Uri: https://archibus.vodacom.co.za/_Incapsula_Resource?CWUDNSAI=23&xinfo=11-124742921-0%200NNN%20RT%2816919534170 46%202308%29%20q%280%20-1%20-1%200%29%20r%280%20-1%29%20B15%284%2C200%2C0%29%20U18&incident_id=128000730324386403-607342817005539915&edet=15&cinfo=04000000&rpinfo=0&mth=GET
Match: pan>

Powered by
Imperva

</body></html>

Uri: https://archibus.vodacom.co.za/_Incapsula_Resource?CWUDNSAI=23&xinfo=59-13731742-0%200NNN%20RT%2817052589557 12%202737%29%20q%280%20-1%20-1%201%29%20r%280%20-1%29%20B15%284%2C200%2C0%29%20U18&incident_id=1686000040225142581-78665255304429883&edet=15&cinfo=04000000&rpinfo=0&mth=GET
Match: pan>

Powered by
Imperva

</body></html>

Uri: https://archibus.vodacom.co.za/_Incapsula_Resource?CWUDNSAI=23&xinfo=6-27452916-0%200NNN%20RT%2816865105732 18%202872%29%20q%280%20-1%20-1%200%29%20r%280%20-1%29%20B15%284%2C200%2C0%29%20U18&incident_id=1367000740168088542-142044571547144838&edet=15&cinfo=04000000&rpinfo=0&mth=GET
Match: pan>

Powered by
Imperva

</body></html>

Uri: https://archibus.vodacom.co.za/_Incapsula_Resource?CWUDNSAI=23&xinfo=6-50760056-0%200NNN%20RT%2816919534055 61%209192%29%20q%280%20-1%20-1%200%29%20r%280%20-1%29%20B15%284%2C200%2C0%29%20U18&incident_id=128000730324386403-257285652188500550&edet=15&cinfo=04000000&rpinfo=0&mth=GET
Match: pan>

Powered by
Imperva

</body></html>

Uri: https://archibus.vodacom.co.za/_Incapsula_Resource?CWUDNSAI=23&xinfo=6-87530002-0%200NNN%20RT%281702234929023%2013%29%20q%280%20-1%20-1%20-1%29%20r%280%20-1%29%20B15%284%2C200%2C0%29%20U18&incident_id=281001070577460321-492085024575265478&edet=15&cinfo=04000000&rpinfo=0&mth=GET
Match: pan>

Powered by
Imperva

</body></html>

Uri: https://archibus.vodacom.co.za/_Incapsula_Resource?CWUDNSAI=23&xinfo=7-38318934-0%200NNN%20RT%281684090979688%2011%29%20q%280%20-1%20-1%20-1%29%20r%280%20-1%29%20B15%284%2C200%2C0%29%20U18&incident_id=765001090170903434-178457729444944711&edet=15&cinfo=04000000&rpinfo=0&mth=GET
Match: pan>

Powered by
Imperva

</body></html>

Uri: https://archibus.vodacom.co.za/_Incapsula_Resource?CWUDNSAI=23&xinfo=7-38798582-0%200NNN%20RT%281686510573218%2015874%29%20q%280%20-1%20-1%200%29%20r%280%20-1%29%20B15%284%2C200%2C0%29%20U18&incident_id=1367000740168088542-199373631805395591&edet=15&cinfo=04000000&rpinfo=0&mth=GET
Match: pan>

Powered by
Imperva

</body></html>

Uri: https://archibus.vodacom.co.za/_Incapsula_Resource?CWUDNSAI=23&xinfo=7-45312741-0%200NNN%20RT%281696791776969%2011%29%20q%280%20-1%20-1%20-1%29%20r%280%20-1%29%20B15%284%2C200%2C0%29%20U18&incident_id=766001150280311651-263255351829077191&edet=15&cinfo=04000000&rpinfo=0&mth=GET
Match: pan>

Powered by
Imperva

</body></html>

Uri: https://archibus.vodacom.co.za/_Incapsula_Resource?CWUDNSAI=23&xinfo=7-68982489-0%200NNN%20RT%281691953407964%203%29%20q%280%20-1%20-1%200%29%20r%280%20-1%29%20B15%284%2c200%2c0%29%20U18&incident_id=128000730324386403-342838544571568711&edet=15&cinfo=04000000&rpinfo=0&mth=GET
Match: pan>

Powered by
Imperva

</body></html>

Uri: https://archibus.vodacom.co.za/_Incapsula_Resource?CWUDNSAI=23&xinfo=7-45312743-0%200NNN%20RT%281696791776989%202667%29%20q%280%20-1%20-1%200%29%20r%280%20-1%29%20B15%284%2C200%2C0%29%20U18&incident_id=766001150280311651-263256700448808135&edet=15&cinfo=04000000&rpinfo=0&mth=GET
Match: pan>

Powered by
Imperva

</body></html>

Uri: https://archibus.vodacom.co.za/_Incapsula_Resource?CWUDNSAI=23&xinfo=8-33065898-0%200NNN%20RT%2816840909760 99%204%29%20q%280%20-1%20-1%20-1%29%20r%280%20-1%29%20B15%284%2c200%2c0%29%20U18&incident_id=765001090170903434-1559182221118738 64&edet=15&cinfo=04000000&rpinfo=0&mth=GET
Match: pan>

Powered by
Imperva

</body></html>

Uri: https://archibus.vodacom.co.za/_Incapsula_Resource?CWUDNSAI=23&xinfo=7-88977006-0%200NNN%20RT%2816999815725061%204262%29%20q%280%20-1%20-1%202%29%20r%280%20-1%29%20B15%284%2C200%2C0%29%20U18&incident_id=767000500460857534-474268430816447623&edet=15&cinfo=04000000&rpinfo=0&mth=GET
Match: pan>

Powered by
Imperva

</body></html>

Uri: https://archibus.vodacom.co.za/_Incapsula_Resource?CWUDNSAI=23&xinfo=7-77442269-0%200NNN%20RT%2816943725301 58%203%29%20q%280%20-1%20-1%201%29%20r%280%20-1%29%20B15%284%2c200%2c0%29%20U18&incident_id=765000070362200247-368447231281136071&edet=15&cinfo=04000000&rpinfo=0&mth=GET
Match: pan>

Powered by
Imperva

</body></html>

Uri: https://archibus.vodacom.co.za/_Incapsula_Resource?CWUDNSAI=23&xinfo=8-63633300-0%200NNN%20RT%2816810668948 08%202364%29%20q%280%20-1%20-1%200%29%20r%280%20-1%29%20B15%284%2c200%2c0%29%20U18&incident_id=451000960203949962-322517894674192392&edet=15&cinfo=04000000&rpinfo=0&mth=GET
Match: pan>

Powered by
Imperva

</body></html>

Uri: https://archibus.vodacom.co.za/_Incapsula_Resource?CWUDNSAI=23&xinfo=8-63631571-0%200NNN%20RT%2816810668741 98%203%29%20q%280%20-1%20-1%20-1%29%20r%280%20-1%29%20B15%284%2c200%2c0%29%20U18&incident_id=451000960203949962-322508943962347528&edet=15&cinfo=04000000&rpinfo=0&mth=GET
Match: pan>

Powered by
Imperva

</body></html>

Uri: https://archibus.vodacom.co.za/_Incapsula_Resource?CWUDNSAI=23&xinfo=8-63633300-0%200NNN%20RT%2816810668948 08%202364%29%20q%280%20-1%20-1%200%29%20r%280%20-1%29%20B15%284%2C200%2C0%29%20U18&incident_id=451000960203949962-322517894674192392&edet=15&cinfo=04000000&rpinfo=0&mth=GET
Match: pan>

Powered by
Imperva

</body></html>

Uri: https://archibus.vodacom.co.za/_Incapsula_Resource?CWUDNSAI=23&xinfo=9-55871876-0%200NNN%20RT%2816865105824 39%205%29%20q%280%20-1%20-1%201%29%20r%280%20-1%29%20B15%284%2c200%2c0%29%20U18&incident_id=1367000740168088542-281164046937821833&edet=15&cinfo=04000000&rpinfo=0&mth=GET
Match: pan>

Powered by
Imperva

</body></html>

Uri: https://archibus.vodacom.co.za/_Incapsula_Resource?CWUDNSAI=23&xinfo=8-71774864-0%200NNN%20RT%2816919533986 94%2013%29%20q%280%20-1%20-1%20-1%29%20r%280%20-1%29%20B15%284%2C200%2C0%29%20U18&incident_id=128000730324386403-355338754828800584&edet=15&cinfo=04000000&rpinfo=0&mth=GET
Match: pan>

Powered by
Imperva

</body></html>

Uri: https://archibus.vodacom.co.za/_Incapsula_Resource?CWUDNSAI=23&xinfo=9-55870156-0%200NNN%20RT%281686510573200%209%29%20q%280%20-1%20-1%20-1%29%20r%280%20-1%29%20B15%284%2C200%2C0%29%20U18&incident_id=1367000740168088542-28115535821898 2025&edet=15&cinfo=04000000&rpinfo=0&mth=GET
Match: pan>

Powered by
Imperva

</body></html>

Uri: https://archibus.vodacom.co.za/_Incapsula_Resource?CWUDNSAI=23&xinfo=9-89541750-0%200NNN%20RT%2816810668948 09%2015180%29%20q%280%20-1%20-1%200%29%20r%280%20-1%29%20B15%284%2c200%2c0%29%20U18&incident_id=451000960203949962-436656818069116937&edet=15&cinfo=04000000&rpinfo=0&mth=GET
Match: pan>

Powered by
Imperva

</body></html>

Uri: https://archibus.vodacom.co.za/_Incapsula_Resource?CWUDNSAI=23&xinfo=9-89541750-0%200NNN%20RT%2816810668948 09%2015180%29%20q%280%20-1%20-1%200%29%20r%280%20-1%29%20B15%284%2C200%2C0%29%20U18&incident_id=451000960203949962-436656818069116937&edet=15&cinfo=04000000&rpinfo=0&mth=GET
Match: pan>

Powered by
Imperva

</body></html>

Uri: https://archibus.vodacom.co.za/_Incapsula_Resource?CWUDNSAI=23&xinfo=11-140064347-0%200NNN%20RT%281702234929044%203123%29%20q%280%20-1%20-1%201%29%20r%280%20-1%29%20B15%284%2C200%2C0%29%20U18&incident_id=281001070577460321-7532348373567474 67&edet=15&cinfo=04000000&rpinfo=0&mth=GET
Match: pan>

Powered by
Imperva

</body></html>

Uri: https://archibus.vodacom.co.za/_Incapsula_Resource?CWUDNSAI=23&xinfo=11-140053216-0%200NNN%20RT%281702234866406%206%29%20q%280%20-1%20-1%20-1%29%20r%280%20-1%29%20B15%284%2c200%2c0%29%20U18&incident_id=281001070577460321-7531738144614058 99&edet=15&cinfo=04000000&rpinfo=0&mth=GET
Match: pan>

Powered by
Imperva

</body></html>

Uri: https://archibus.vodacom.co.za/_Incapsula_Resource?CWUDNSAI=23&xinfo=11-140064348-0%200NNN%20RT%281702234929044%2016190%29%20q%280%20-1%20-1%202%29%20r%280%20-1%29%20B15%284%2C200%2C0%29%20U18&incident_id=281001070577460321-7532465368476617 71&edet=15&cinfo=04000000&rpinfo=0&mth=GET
Match: pan>

Powered by
Imperva

</body></html>

Uri: https://archibus.vodacom.co.za/_Incapsula_Resource?CWUDNSAI=23&xinfo=12-133842840-0%200NNN%20RT%281699815708995%2011%29%20q%280%20-1%20-1%20-1%29%20r%280%20-1%29%20B15%284%2C200%2C0%29%20U18&incident_id=767000500460857534-7089520452346215 80&edet=15&cinfo=04000000&rpinfo=0&mth=GET
Match: pan>

Powered by
Imperva

</body></html>

Uri: https://archibus.vodacom.co.za/_Incapsula_Resource?CWUDNSAI=23&xinfo=12-133841466-0%200NNN%20RT%281699815698488%205%29%20q%280%20-1%20-1%20-1%29%20r%280%20-1%29%20B15%284%2c200%2c0%29%20U18&incident_id=767000500460857534-7089442155092409 72&edet=15&cinfo=04000000&rpinfo=0&mth=GET
Match: pan>

Powered by
Imperva

</body></html>

Uri: https://archibus.vodacom.co.za/_Incapsula_Resource?CWUDNSAI=23&xinfo=12-143392341-0%200NNN%20RT%281691953401023%20467%29%20q%280%20-1%20-1%201%29%20r%280%20-1%29%20B15%284%2C200%2C0%29%20U18&incident_id=128000730324386403-6886819771040446 20&edet=15&cinfo=04000000&rpinfo=0&mth=GET
Match: pan>

Powered by
Imperva

</body></html>

Uri: https://archibus.vodacom.co.za/_Incapsula_Resource?CWUDNSAI=23&xinfo=12-77124096-0%200NNN%20RT%281684090979706%202875%29%20q%280%20-1%20-1%200%29%20r%280%20-1%29%20B15%284%2C200%2C0%29%20U18&incident_id=765001090170903434-359187810071944012&edet=15&cinfo=04000000&rpinfo=0&mth=GET
Match: pan>

Powered by
Imperva

</body></html>

Uri: https://archibus.vodacom.co.za/_Incapsula_Resource?CWUDNSAI=23&xinfo=12-182571436-0%200NNN%20RT%281688929427753%2015665%29%20q%280%20-1%20-1%202%29%20r%280%20-1%29%20B15%284%2C200%2C0%29%20U18&incident_id=763001020386100101-868537211589171596&edet=15&cinfo=04000000&rpinfo=0&mth=GET
Match: pan>

Powered by
Imperva

</body></html>

Uri: https://archibus.vodacom.co.za/_Incapsula_Resource?CWUDNSAI=23&xinfo=12-95056015-0%200NNN%20RT%281686510510454%2011%29%20q%280%20-1%20-1%20-1%29%20r%280%20-1%29%20B15%284%2c200%2c0%29%20U18&incident_id=1367000740168088542-463133393133441676&edet=15&cinfo=04000000&rpinfo=0&mth=GET
Match: pan>

Powered by
Imperva

</body></html>

Uri: https://archibus.vodacom.co.za/_Incapsula_Resource?CWUDNSAI=23&xinfo=13-145678257-0%200NNN%20RT%281694372520934%2012%29%20q%280%20-1%20-1%20-1%29%20r%280%20-1%29%20B15%284%2C200%2C0%29%20U18&incident_id=765000070362200247-690227250544312781&edet=15&cinfo=04000000&rpinfo=0&mth=GET
Match: pan>

Powered by
Imperva

</body></html>

Uri: https://archibus.vodacom.co.za/_Incapsula_Resource?CWUDNSAI=23&xinfo=12-77127187-0%200NNN%20RT%281684090995888%204094%29%20q%280%20-1%20-1%200%29%20r%280%20-1%29%20B15%284%2C200%2C0%29%20U18&incident_id=765001090170903434-359203417983097676&edet=15&cinfo=04000000&rpinfo=0&mth=GET
Match: pan>

Powered by
Imperva

</body></html>

Uri: https://archibus.vodacom.co.za/_Incapsula_Resource?CWUDNSAI=23&xinfo=13-146013152-0%200NNN%20RT%281699815709015%202793%29%20q%280%20-1%20-1%204%29%20r%280%20-1%29%20B15%284%2C200%2C0%29%20U18&incident_id=767000500460857534-774752327188810893&edet=15&cinfo=04000000&rpinfo=0&mth=GET
Match: pan>

Powered by
Imperva

</body></html>

Uri: https://archibus.vodacom.co.za/_Incapsula_Resource?CWUDNSAI=23&xinfo=13-157825945-0%200NNN%20RT%281691953421567%2015799%29%20q%280%20-1%20-1%201%29%20r%280%20-1%29%20B15%284%2C200%2C0%29%20U18&incident_id=128000730324386403-757535280726020685&edet=15&cinfo=04000000&rpinfo=0&mth=GET
Match: pan>

Powered by
Imperva

</body></html>

Uri: https://archibus.vodacom.co.za/_Incapsula_Resource?CWUDNSAI=23&xinfo=13-146014798-0%200NNN%20RT%281699815718661%203%29%20q%280%20-1%20-1%200%29%20r%280%20-1%29%20B15%284%2c200%2c0%29%20U18&incident_id=767000500460857534-774758262833613965&edet=15&cinfo=04000000&rpinfo=0&mth=GET
Match: pan>

Powered by
Imperva

</body></html>

Uri: https://archibus.vodacom.co.za/_Incapsula_Resource?CWUDNSAI=23&xinfo=13-165603926-0%200NNN%20RT%2816888929427724%2020%29%20q%280%20-1%20-1%20-1%29%20r%280%20-1%29%20B15%284%2C200%2C0%29%20U18&incident_id=763001020386100101-784253361782987149&edet=15&cinfo=04000000&rpinfo=0&mth=GET
Match: pan>

Powered by
Imperva

</body></html>

Uri: https://archibus.vodacom.co.za/_Incapsula_Resource?CWUDNSAI=23&xinfo=13-70581997-0%200NNN%20RT%281696791714311%206%29%20q%280%20-1%20-1%20-1%29%20r%280%20-1%29%20B15%284%2c200%2c0%29%20U18&incident_id=766001150280311651-392143205803367629&edet=15&cinfo=04000000&rpinfo=0&mth=GET
Match: pan>

Powered by
Imperva

</body></html>

Uri: https://archibus.vodacom.co.za/_Incapsula_Resource?CWUDNSAI=23&xinfo=13-70594367-0%200NNN%20RT%281696791792934%204590%29%20q%280%20-1%20-1%200%29%20r%280%20-1%29%20B15%284%2C200%2C0%29%20U18&incident_id=766001150280311651-392210022609591501&edet=15&cinfo=04000000&rpinfo=0&mth=GET
Match: pan>

Powered by
Imperva

</body></html>

Uri: https://archibus.vodacom.co.za/_Incapsula_Resource?CWUDNSAI=23&xinfo=13-85261504-0%200NNN%20RT%281684090989049%203%29%20q%280%20-1%20-1%2059%29%20r%281%20-1%29%20B15%284%2c200%2c0%29%20U18&incident_id=765001090170903434-393561803436399437&edet=15&cinfo=04000000&rpinfo=0&mth=GET
Match: pan>

Powered by
Imperva

</body></html>

Uri: https://archibus.vodacom.co.za/_Incapsula_Resource?CWUDNSAI=23&xinfo=14-163458765-0%200NNN%20RT%281694372517397%203%29%20q%280%20-1%20-1%20-1%29%20r%281%20-1%29%20B15%284%2c200%2c0%29%20U18&incident_id=765000070362200247-772768924176286158&edet=15&cinfo=04000000&rpinfo=0&mth=GET
Match: pan>

Powered by
Imperva

</body></html>

Uri: https://archibus.vodacom.co.za/_Incapsula_Resource?CWUDNSAI=23&xinfo=14-114596260-0%200NNN%20RT%281686510589098%204193%29%20q%280%20-1%20-1%203%29%20r%280%20-1%29%20B15%284%2C200%2C0%29%20U18&incident_id=1367000740168088542-54786852803831873 4&edet=15&cinfo=04000000&rpinfo=0&mth=GET
Match: pan>

Powered by
Imperva

</body></html>

Uri: https://archibus.vodacom.co.za/_Incapsula_Resource?CWUDNSAI=23&xinfo=14-163459825-0%200NNN%20RT%281694372520953%202886%29%20q%280%20-1%20-1%200%29%20r%280%20-1%29%20B15%284%2C200%2C0%29%20U18&incident_id=7650000703622002 47-772776844095979982&edet=15&cinfo=04000000&rpinfo=0&mth=GET
Match: pan>

Powered by
Imperva

</body></html>

Uri: https://archibus.vodacom.co.za/_Incapsula_Resource?CWUDNSAI=23&xinfo=14-98161412-0%200NNN%20RT%281684090979710%2016171%29%20q%280%20-1%20-1%200%29%20r%280%20-1%29%20B15%284%2C200%2C0%29%20U18&incident_id=7650010901709034 34-451351309958585166&edet=15&cinfo=04000000&rpinfo=0&mth=GET
Match: pan>

Powered by
Imperva

</body></html>

Uri: https://archibus.vodacom.co.za/_Incapsula_Resource?CWUDNSAI=23&xinfo=2-16530192-0%200NNN%20RT%281696791776989%2015936%29%20q%280%20-1%20-1%200%29%20r%280%20-1%29%20B15%284%2C200%2C0%29%20U18&incident_id=7660011502803116 51-85428939677113538&edet=15&cinfo=04000000&rpinfo=0&mth=GET
Match: pan>

Powered by
Imperva

</body></html>

Uri: https://archibus.vodacom.co.za/_Incapsula_Resource?CWUDNSAI=23&xinfo=2-26051945-0%200NNN%20RT%281694372536840%204197%29%20q%280%20-1%20-1%200%29%20r%280%20-1%29%20B15%284%2C200%2C0%29%20U18&incident_id=7650000703622002 47-129321293534003650&edet=15&cinfo=04000000&rpinfo=0&mth=GET

Match: pan>

Powered by
Imperva

</body></html>

Uri: https://archibus.vodacom.co.za/_Incapsula_Resource?CWUDNSAI=23&xinfo=31-5366570-0%200NNN%20RT%281705258918883%203%29%20q%280%20-1%20-1%20-1%29%20r%280%20-1%29%20B15%284%2c200%2c0%29%20U18&incident_id=1686000040225142581-31032581933105439&edet=15&cinfo=04000000&rpinfo=0&mth=GET
Match: pan>

Powered by
Imperva

</body></html>

Uri: https://archibus.vodacom.co.za/_Incapsula_Resource?CWUDNSAI=23&xinfo=3-53041329-0%200NNN%20RT%281702234945242%204178%29%20q%280%20-1%20-1%200%29%20r%280%20-1%29%20B15%284%2C200%2C0%29%20U18&incident_id=281001070577460321-31370405913094419 5&edet=15&cinfo=04000000&rpinfo=0&mth=GET
Match: pan>

Powered by
Imperva

</body></html>

Uri: https://archibus.vodacom.co.za/_Incapsula_Resource?CWUDNSAI=23&xinfo=32-11389906-0%200NNN%20RT%281705258971756%204195%29%20q%280%20-1%20-1%201%29%20r%280%20-1%29%20B15%284%2C200%2C0%29%20U18&incident_id=1686000040225142581-65795549010723104&edet=15&cinfo=04000000&rpinfo=0&mth=GET
Match: pan>

Powered by
Imperva

</body></html>

Uri: https://archibus.vodacom.co.za/_Incapsula_Resource?CWUDNSAI=23&xinfo=4-38615588-0%200NNN%20RT%281696791786552%208%29%20q%280%20-1%20-1%200%29%20r%280%20-1%29%20B15%284%2c200%2c0%29%20U18&incident_id=766001150280311651-20106118025118432 4&edet=15&cinfo=04000000&rpinfo=0&mth=GET
Match: pan>

Powered by

Imperva

</body></html>

Uri: https://archibus.vodacom.co.za/_Incapsula_Resource?CWUDNSAI=23&xinfo=37-6911038-0%200NNN%20RT%281705258955691%2015%29%20q%280%20-1%20-1%20-1%29%20r%280%20-1%29%20B15%284%2C200%2C0%29%20U18&incident_id=1686000040225142581-40508744371929381&edet=15&cinfo=04000000&rpinfo=0&mth=GET
Match: pan>

Powered by
Imperva

</body></html>

Uri: https://archibus.vodacom.co.za/_Incapsula_Resource?CWUDNSAI=23&xinfo=5-109279300-0%200NNN%20RT%281681066903598%208%29%20q%280%20-1%20-1%201%29%20r%280%20-1%29%20B15%284%2c200%2c0%29%20U18&incident_id=45100960203949962-52894951057202176 5&edet=15&cinfo=04000000&rpinfo=0&mth=GET
Match: pan>

Powered by
Imperva

</body></html>

Uri: https://archibus.vodacom.co.za/_Incapsula_Resource?CWUDNSAI=23&xinfo=5-116739429-0%200NNN%20RT%281688929427752%202697%29%20q%280%20-1%20-1%200%29%20r%280%20-1%29%20B15%284%2C200%2C0%29%20U18&incident_id=763001020386100101-555576851833756037&edet=15&cinfo=04000000&rpinfo=0&mth=GET
Match: pan>

Powered by
Imperva

</body></html>

Uri: https://archibus.vodacom.co.za/_Incapsula_Resource?CWUDNSAI=23&xinfo=5-116740391-0%200NNN%20RT%281688929436725%203%29%20q%280%20-1%20-1%200%29%20r%280%20-1%29%20B15%284%2c200%2c0%29%20U18&incident_id=763001020386100101-555579935620274565&edet=15&cinfo=04000000&rpinfo=0&mth=GET
Match: pan>

Powered by
Imperva

</body></html>

Uri: https://archibus.vodacom.co.za/_Incapsula_Resource?CWUDNSAI=23&xinfo=5-116741115-0%200NNN%20RT%281688929443426%204203%29%20q%280%20-1%20-1%200%29%20r

%280%20-1%29%20B15%284%2C200%2C0%29%20U18&incident_id=763001020386100101-555585841200306565&edet=15&cinfo=04000000&rpinfo=0&mth=GET
Match: pan>

Powered by
Imperva

</body></html>

Total 561 request(s) were blocked by WAF/IPS/Firewall during path manipulation testing.Total 561 request(s) were blocked by WAF/IPS/Firewall during path manipulation testing.Total 562 request(s) were blocked by WAF/IPS/Firewall during path manipulation testing.Total 563 request(s) were blocked by WAF/IPS/Firewall during path manipulation testing.Total 564 request(s) were blocked by WAF/IPS/Firewall during path manipulation testing.Total 565 request(s) were blocked by WAF/IPS/Firewall during path manipulation testing.

150116 Server Authentication Found (1)

150116 Server Authentication Found

archibus.vodacom.co.za:443/fpr/index.as

Finding #	14173442	**Severity**	Information Gathered - Level 1
Unique #	d182b92d-6fd0-44ad-b2fd-05e1aff98218		
Group	Scan Diagnostics		
CWE	-	**Detection Date**	11 Feb 2024 21:02 GMT+0200
OWASP	-		
WASC	-		

Details

Threat

Server Authentication was found during the web application crawling.

Impact

N/A

Solution

N/A

Results

Server authentication found:
Url: https://archibus.vodacom.co.za/FPRWin/index.aspx
Type: unknown
Server authentication found:
Url: https://archibus.vodacom.co.za/FPRWin/index.aspx
Type: NTLM

150152 Forms Crawled (1)

150152 Forms Crawled

archibus.vodacom.co.za:443/fpr/index.as

Finding #	10510208	**Severity**	Information Gathered - Level 1
Unique #	c2e814ae-9d23-4e0d-995c-2b9b324dd3bb		
Group	Scan Diagnostics		
CWE	-	**Detection Date**	11 Feb 2024 21:02 GMT+0200
OWASP	-		
WASC	-		

Details

Threat
The Results section lists the unique forms that were identified and submitted by the scanner. The forms listed in this QID do not include authentication forms (i.e. login forms), which are reported separately under QID 150115.

The scanner does a redundancy check on forms by inspecting the form fields. Forms determined to be the redundant based on identical form fields will not be tested. If desired, you can enable 'Include form action URI in form uniqueness calculation' in the WAS option profile to have the scanner also consider the form's action attribute in the redundancy check.

NOTE: Any regular expression specified under 'Redundant Links' are not applied to forms. Forms (unique or redundant) are not reported under QID 150140.

Impact
N/A

Solution
N/A

Results

Total internal forms seen (this count includes duplicate forms): 0

Crawled forms (Total: 0)
NOTE: This does not include authentication forms. Authentication forms are reported separately in QID 150115

150172 Requests Crawled (1)

150172 Requests Crawled — *archibus.vodacom.co.za:443/fpr/index.as*

Finding #	10510222	**Severity**	Information Gathered - Level 1
Unique #	00bcec2d-4ef0-4e5e-822f-524c4465b43a		
Group	Scan Diagnostics		
CWE	-	**Detection Date**	11 Feb 2024 21:02 GMT+0200
OWASP	-		
WASC	-		

Details

Threat
The QID reports list of requests crawled by the Web application scanner appear in the Results section.

Impact
N/A

Solution
N/A

Results

Number of crawled XHRs (XHRs, Fetch and External XHRs): 118

Fetch Requests: 118
Method POST URI https://archibus.vodacom.co.za/Leasure-the-deed-will-the-clipt-Angely-ands-Banq?d=archibus.vodacom.co.za (Count: 118)

WAS Web Application Report

150247 Web Server and Technologies Detected (1)

150247 Web Server and Technologies Detected

archibus.vodacom.co.za:443/fpr/index.as

Finding #	14173441	**Severity**	Information Gathered - Level 1
Unique #	c7a1a598-0947-4184-a2f9-49217b659516		
Group	Scan Diagnostics		
CWE	CWE-200	**Detection Date**	11 Feb 2024 21:02 GMT+0200
OWASP	-		
WASC	-		

Details

Threat

Information disclosure is an application weakness in revealing sensitive data, such as technical details of the system or environment.

This check reports the various technologies used by the web application based on the information available in different components of the Request-Response.

Impact

An attacker may use sensitive data to exploit the target web application, its hosting network, or its users.

Solution

Ensure that your web servers do not reveal any sensitive information about your technology stack and system details

Please review the issues reported below:

Results

Number of technologies detected: 2
Technology name: Microsoft ASP.NET
Matched Components:
header match:
X-Powered-By:ASP.NET
Matched links: reporting only first 3 links
https://archibus.vodacom.co.za/FPRWin/
https://archibus.vodacom.co.za/FPRWin/index.aspx

Technology name: Microsoft IIS
Technology version: Microsoft IIS 10.0
Matched Components:
header match:
Server:Microsoft-IIS/10.0
Matched links: reporting only first 3 links
https://archibus.vodacom.co.za/FPRWin/
https://archibus.vodacom.co.za/FPRWin/index.aspx

150528 Server Returns HTTP 4XX Error Code During Scanning (1)

150528 Server Returns HTTP 4XX Error Code During Scanning

archibus.vodacom.co.za:443/fpr/index.as

Finding #	10510002	**Severity**	Information Gathered - Level 1
Unique #	d3c8feed-cbc2-4089-aa7b-fcab9b83f672		
Group	Scan Diagnostics		
CWE	-	**Detection Date**	11 Feb 2024 21:02 GMT+0200
OWASP	-		
WASC	-		

WAS Web Application Report

Details

Threat

During the WAS scan, links with HTTP 4xx response code were observed and these are listed in the Results section. The HTTP 4xx message indicates a client error. The list of supported 4xx response code are as below:

400 - Bad Request
401 - Unauthorized
403 - Forbidden
404 - Not Found
405 - Method Not Allowed
407 - Proxy Authentication Required
408 - Request Timeout
413 - Payload Too Large
414 - URI Too Long

Impact

The presence of a HTTP 4xx error during the crawl phase indicates that some problem exists on the website that will be encountered during normal usage of the Web application. Note WAS depends on responses to detect many vulnerabilities if the link does not respond with an expected response then any vulnerabilities present on such links may not be detected.

Solution

Review each link to determine why the client encountered an error while requesting the link. Additionally review and investigate the results of QID 150042 which lists 5xx errors, QID 150019 which lists unexpected response codes and QID 150097 which lists a potential blocked request.

Results

Number of links with 4xx response code: 60
(Only first 50 such links are listed)

401 https://archibus.vodacom.co.za/FPRWin/
401 https://archibus.vodacom.co.za/FPRWin/index.aspx
404 https://archibus.vodacom.co.za/_Incapsula_Resource?CWUDNSAI=23%22xinfo=1-22384977-0%200NNN%20RT%2816998157090 16%2016037%29%20q%280%20-1%20-1%200%29%20r%280%20-1%29%20B15%284%2c200%2c0%29%20U18%22incident_id=76700050046085753 4-122447288571202689%22edet=15%22cinfo=04000000%22rpinfo=0%22mth=GET
404 https://archibus.vodacom.co.za/_Incapsula_Resource?CWUDNSAI=23%22xinfo=11-111956721-0%200NNN%20RT%2816943725209 54%2015878%29%20q%280%20-1%20-1%200%29%20r%280%20-1%29%20B15%284%2c200%2c0%29%20U18%22incident_id=76500007036220024 7-534536421231100363%22edet=15%22cinfo=04000000%22rpinfo=0%22mth=GET
404 https://archibus.vodacom.co.za/_Incapsula_Resource?CWUDNSAI=23%22xinfo=11-124742921-0%200NNN%20RT%2816919534170 46%202308%29%20q%280%20-1%20-1%200%29%20r%280%20-1%29%20B15%284%2c200%2c0%29%20U18%22incident_id=12800073032438640 3-607342817005539915%22edet=15%22cinfo=04000000%22rpinfo=0%22mth=GET
404 https://archibus.vodacom.co.za/_Incapsula_Resource?CWUDNSAI=23%22xinfo=11-140064347-0%200NNN%20RT%2817022349290 44%203123%29%20q%280%20-1%20-1%201%29%20r%280%20-1%29%20B15%284%2c200%2c0%29%20U18%22incident_id=28100107057746032 1-753234837356747467%22edet=15%22cinfo=04000000%22rpinfo=0%22mth=GET
404 https://archibus.vodacom.co.za/_Incapsula_Resource?CWUDNSAI=23%22xinfo=11-140064348-0%200NNN%20RT%2817022349290 44%2016190%29%20q%280%20-1%20-1%202%29%20r%280%20-1%29%20B15%284%2c200%2c0%29%20U18%22incident_id=28100107057746032 1-753246536847661771%22edet=15%22cinfo=04000000%22rpinfo=0%22mth=GET
404 https://archibus.vodacom.co.za/_Incapsula_Resource?CWUDNSAI=23%22xinfo=12-143392341-0%200NNN%20RT%2816919534010 23%20467%29%20q%280%20-1%20-1%201%29%20r%280%20-1%29%20B15%284%2c200%2c0%29%20U18%22incident_id=12800073032438640 3-688681977104044620%22edet=15%22cinfo=04000000%22rpinfo=0%22mth=GET
404 https://archibus.vodacom.co.za/_Incapsula_Resource?CWUDNSAI=23%22xinfo=12-182571436-0%200NNN%20RT%2816889294275 53%2015665%29%20q%280%20-1%20-1%202%29%20r%280%20-1%29%20B15%284%2c200%2c0%29%20U18%22incident_id=76300102038610010 1-868537211589171596%22edet=15%22cinfo=04000000%22rpinfo=0%22mth=GET
404 https://archibus.vodacom.co.za/_Incapsula_Resource?CWUDNSAI=23%22xinfo=12-77124096-0%200NNN%20RT%2816840909797 06%202875%29%20q%280%20-1%20-1%200%29%20r%280%20-1%29%20B15%284%2c200%2c0%29%20U18%22incident_id=76500109017090343 4-359187810071944012%22edet=15%22cinfo=04000000%22rpinfo=0%22mth=GET
404 https://archibus.vodacom.co.za/_Incapsula_Resource?CWUDNSAI=23%22xinfo=12-77127187-0%200NNN%20RT%2816840909958 88%204094%29%20q%280%20-1%20-1%200%29%20r%280%20-1%29%20B15%284%2c200%2c0%29%20U18%22incident_id=76500109017090343 4-359203417983097676%22edet=15%22cinfo=04000000%22rpinfo=0%22mth=GET
404 https://archibus.vodacom.co.za/_Incapsula_Resource?CWUDNSAI=23%22xinfo=13-146013152-0%200NNN%20RT%2816998157090 15%202793%29%20q%280%20-1%20-1%204%29%20r%280%20-1%29%20B15%284%2c200%2c0%29%20U18%22incident_id=76700050046085753 4-774752327188810893%22edet=15%22cinfo=04000000%22rpinfo=0%22mth=GET
404 https://archibus.vodacom.co.za/_Incapsula_Resource?CWUDNSAI=23%22xinfo=13-157825945-0%200NNN%20RT%2816919534215 67%2015799%29%20q%280%20-1%20-1%201%29%20r%280%20-1%29%20B15%284%2c200%2c0%29%20U18%22incident_id=12800073032438640 3-757535280726020685%22edet=15%22cinfo=04000000%22rpinfo=0%22mth=GET
404 https://archibus.vodacom.co.za/_Incapsula_Resource?CWUDNSAI=23%22xinfo=13-70594367-0%200NNN%20RT%2816967917929 34%204590%29%20q%280%20-1%20-1%200%29%20r%280%20-1%29%20B15%284%2c200%2c0%29%20U18%22incident_id=76600115028031165 1-392210022609591501%22edet=15%22cinfo=04000000%22rpinfo=0%22mth=GET
404 https://archibus.vodacom.co.za/_Incapsula_Resource?CWUDNSAI=23%22xinfo=14-114596260-0%200NNN%20RT%2816865105890 98%204193%29%20q%280%20-1%20-1%203%29%20r%280%20-1%29%20B15%284%2c200%2c0%29%20U18%22incident_id=13670007401680885 42-5478685280383187 34%22edet=15%22cinfo=04000000%22rpinfo=0%22mth=GET
404 https://archibus.vodacom.co.za/_Incapsula_Resource?CWUDNSAI=23%22xinfo=14-163459825-0%200NNN%20RT%2816943725209 53%202886%29%20q%280%20-1%20-1%200%29%20r%280%20-1%29%20B15%284%2c200%2c0%29%20U18%22incident_id=76500007036220024 7-772776844095979982%22edet=15%22cinfo=04000000%22rpinfo=0%22mth=GET
404 https://archibus.vodacom.co.za/_Incapsula_Resource?CWUDNSAI=23%22xinfo=14-98161412-0%200NNN%20RT%2816840909797 10%2016171%29%20q%280%20-1%20-1%200%29%20r%280%20-1%29%20B15%284%2c200%2c0%29%20U18%22incident_id=76500109017090343 4-451351309958585166%22edet=15%22cinfo=04000000%22rpinfo=0%22mth=GET
404 https://archibus.vodacom.co.za/_Incapsula_Resource?CWUDNSAI=23%22xinfo=2-16530192-0%200NNN%20RT%2816967917769 89%2015936%29%20q%280%20-1%20-1%200%29%20r%280%20-1%29%20B15%284%2c200%2c0%29%20U18%22incident_id=76600115028031165 1-854289396771135 38%22edet=15%22cinfo=04000000%22rpinfo=0%22mth=GET
404 https://archibus.vodacom.co.za/_Incapsula_Resource?CWUDNSAI=23%22xinfo=2-26051945-0%200NNN%20RT%2816943725368 40%204197%29%20q%280%20-1%20-1%200%29%20r%280%20-1%29%20B15%284%2c200%2c0%29%20U18%22incident_id=76500007036220024 7-129321293534003650%22edet=15%22cinfo=04000000%22rpinfo=0%22mth=GET
404 https://archibus.vodacom.co.za/_Incapsula_Resource?CWUDNSAI=23%22xinfo=3-53041329-0%200NNN%20RT%2817022349452 42%204178%29%20q%280%20-1%20-1%200%29%20r%280%20-1%29%20B15%284%2c200%2c0%29%20U18%22incident_id=28100107057746032 1-313704059130944195%22edet=15%22cinfo=04000000%22rpinfo=0%22mth=GET
404 https://archibus.vodacom.co.za/_Incapsula_Resource?CWUDNSAI=23%22xinfo=32-11389906-0%200NNN%20RT%2817052589717 56%204195%29%20q%280%20-1%20-1%201%29%20r%280%20-1%29%20B15%284%2c200%2c0%29%20U18%22incident_id=16860000402251425 81-65795549010723104%22edet=15%22cinfo=04000000%22rpinfo=0%22mth=GET
404 https://archibus.vodacom.co.za/_Incapsula_Resource?CWUDNSAI=23%22xinfo=5-116739429-0%200NNN%20RT%2816888929427752%202697%29%20q%280%20-1%20-1%200%29%20r

%280%20-1%29%20B15%284%2c200%2c0%29%20U18%22incident_id=763001020386100101-555576851833756037%22edet=15%22cinfo=04000000%22rpinfo=0%22mth=GET
404 https://archibus.vodacom.co.za/_Incapsula_Resource?CWUDNSAI=23%22xinfo=5-116741115-0%200NNN%20RT%2816889294434 26%204203%29%20q%280%20-1%20-1%200%29%20r
%280%20-1%29%20B15%284%2c200%2c0%29%20U18%22incident_id=763001020386100101-555585841200306565%22edet=15%22cinfo=04000000%22rpinfo=0%22mth=GET
404 https://archibus.vodacom.co.za/_Incapsula_Resource?CWUDNSAI=23%22xinfo=52-10807422-0%200NNN%20RT%2817052589557 14%2016035%29%20q%280%20-1%20-1%201%29%20r
%280%20-1%29%20B15%284%2c200%2c0%29%20U18%22incident_id=168600004022514 2581-618463609417894 92%22edet=15%22cinfo=04000000%22rpinfo=0%22mth=GET
404 https://archibus.vodacom.co.za/_Incapsula_Resource?CWUDNSAI=23%22xinfo=59-13731742-0%200NNN%20RT%2817052589557 12%202737%29%20q%280%20-1%20-1%201%29%20r
%280%20-1%29%20B15%284%2c200%2c0%29%20U18%22incident_id=168600004022514 2581-786652553044298 83%22edet=15%22cinfo=04000000%22rpinfo=0%22mth=GET
404 https://archibus.vodacom.co.za/_Incapsula_Resource?CWUDNSAI=23%22xinfo=6-27452916-0%200NNN%20RT%2816865105732 18%202872%29%20q%280%20-1%20-1%200%29%20r
%280%20-1%29%20B15%284%2c200%2c0%29%20U18%22incident_id=136700074016808 8542-142044571547144838%22edet=15%22cinfo=04000000%22rpinfo=0%22mth=GET
404 https://archibus.vodacom.co.za/_Incapsula_Resource?CWUDNSAI=23%22xinfo=6-50760056-0%200NNN%20RT%2816919534055 61%209192%29%20q%280%20-1%20-1%200%29%20r
%280%20-1%29%20B15%284%2c200%2c0%29%20U18%22incident_id=128000730324386403-257285652188500550%22edet=15%22cinfo=04000000%22rpinfo=0%22mth=GET
404 https://archibus.vodacom.co.za/_Incapsula_Resource?CWUDNSAI=23%22xinfo=7-45312743-0%200NNN%20RT%2816967917769 89%202667%29%20q%280%20-1%20-1%200%29%20r
%280%20-1%29%20B15%284%2c200%2c0%29%20U18%22incident_id=766001150280311651-263256700448808135%22edet=15%22cinfo=04000000%22rpinfo=0%22mth=GET
404 https://archibus.vodacom.co.za/docs/
404 https://archibus.vodacom.co.za/docs/RELEASE-NOTES.txt
404 https://archibus.vodacom.co.za/docs/api/
404 https://archibus.vodacom.co.za/docs/api/index.html
404 https://archibus.vodacom.co.za/docs/appdev/
404 https://archibus.vodacom.co.za/docs/changelog.html
404 https://archibus.vodacom.co.za/docs/cluster-howto.html
404 https://archibus.vodacom.co.za/docs/config/
404 https://archibus.vodacom.co.za/docs/deployer-howto.html
404 https://archibus.vodacom.co.za/docs/jndi-datasource-examples-howto.html
404 https://archibus.vodacom.co.za/docs/manager-howto.html
404 https://archibus.vodacom.co.za/docs/realm-howto.html
404 https://archibus.vodacom.co.za/docs/security-howto.html
404 https://archibus.vodacom.co.za/docs/setup.html
404 https://archibus.vodacom.co.za/examples/
403 https://archibus.vodacom.co.za/fpr/
404 https://archibus.vodacom.co.za/fpr/index.asp
404 https://archibus.vodacom.co.za/host-manager/
404 https://archibus.vodacom.co.za/host-manager/html
404 https://archibus.vodacom.co.za/manager/
404 https://archibus.vodacom.co.za/manager/html
404 https://archibus.vodacom.co.za/manager/status

150546 First Link Crawled Response Code Information (1)

150546 First Link Crawled Response Code Information

archibus.vodacom.co.za:443/fpr/index.as

Finding #	10510212	**Severity**	Information Gathered - Level 1
Unique #	2de4dd5d-3c53-482f-9b77-9b25ae5581bc		
Group	Scan Diagnostics		
CWE	-	**Detection Date**	11 Feb 2024 21:02 GMT+0200
OWASP	-		
WASC	-		

Details

Threat

The Web server returned the following information from where the Web application scanning engine initiated. Information reported includes First Link Crawled, response Code, response Header, and response Body (first 500 characters). The first link crawled is the "Web Application URL (or Swagger file URL)" set in the Web Application profile.

Impact

An erroneous response might be indicative of a problem in the Web server, or the scan configuration.

Solution

Review the information to check if this is in line with the expected scan configuration. Refer to the output of QIDs 150009, 150019, 150021, 150042 and 150528 (if present) for additional details.

Results

Base URI: https://archibus.vodacom.co.za/fpr/index.asp
Response Code: 404
Response Header:
content-encoding: gzip
content-security-policy-report-only: default-src 'self' 'unsafe-eval' 'unsafe-hashes' 'unsafe-inline' data: blob: ; form-action 'none' data: blob: ; report-uri /csp_report

```
content-type: text/html
date: Sun, 11 Feb 2024 19:03:21 GMT
instance: /ITG/pool_archibus_8080 10.134.16.81 8080
server: Microsoft-IIS/10.0
x-cdn: Imperva
x-frame-options: SAMEORIGIN
x-iinfo: 62-26458618-26458857 NNYY CT(166 165 0) RT(1707678197609 3448) q(0 0 0 -1) r(2 2) U11
x-powered-by: ASP.NET
Set-Cookie: visid_incap_2776849=XzGtDabQTHuVkbHOgCNGXPUZyWUAAAAAQUIPAAAAAABzHTfqgLA/hAMNNToBRAEF; HttpOnly; expires=Sun, 09-Feb-2025 22:21:08 GMT;
domain=.vodacom.co.za; path=/
Set-Cookie: nlbi_2776849=1uvTSns0kGzwA8rXZU49BAAAAABumPnVc6r7kZo+kAK6WiUr; domain=.vodacom.co.za; path=/
Set-Cookie: incap_ses_1687_2776849=ArRnARTRdWEO7PgfvG1pF/UZyWUAAAACho9ich3SZo+8LGHMtIyTQ==; domain=.vodacom.co.za; path=/
Set-Cookie: nlbi_2776849_2147483392=bdxSNQkzDQqTStFxZU49BAAAAACIDUPtWJ8TWiQ58j4j06LA; domain=.vodacom.co.za; path=/

Response Body:
<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Strict//EN" "http://www.w3.org/TR/xhtml1/DTD/xhtml1-strict.dtd"><html xmlns="http://www.w3.org/1999/xhtml"><head><script src="/
Leasure-the-deed-will-the-clipt-Angely-ands-Banq" async=""></script>
<meta http-equiv="Content-Type" content="text/html; charset=iso-8859-1">
<title>404 - File or directory not found.</title>
<style type="text/css">
<!--
body{margin:0;font-size:.7em;font-family:Verdana, Arial, Helvetica, sans-serif;background:#EEEEEE;}
fieldse
...
```

150621 List of JavaScript Links (1)

150621 List of JavaScript Links

archibus.vodacom.co.za:443/fpr/index.as

Finding #	10510224	**Severity**	Information Gathered - Level 1
Unique #	e729b308-88e5-4e69-bcab-0e800ba4886b		
Group	Scan Diagnostics		
CWE	-	**Detection Date**	11 Feb 2024 21:02 GMT+0200
OWASP	-		
WASC	-		

Details

Threat

This QID reports all the JavaScript links that are in-scope of this scan.

Impact

JavaScript links may pose security risks such as XSS, CSRF.

Solution

Verify JavaScript links are intentional and required for your web application.
Review any third party scripts that are hosted on your local server instead of using CDN.
Update all the JavaScript libraries with latest version as applicable.

Results

JavaScript Links were found while crawling.
Total Number of Links: 31
https://archibus.vodacom.co.za/Leasure-the-deed-will-the-clipt-Angely-ands-Banq
https://archibus.vodacom.co.za/_Incapsula_Resource?SWJIYLWA=719d34d31c8e3a6e6fffd425f7e032f3&ns=12&cb=1246061612
https://archibus.vodacom.co.za/_Incapsula_Resource?SWJIYLWA=719d34d31c8e3a6e6fffd425f7e032f3%22ns=7%22cb=650421431
https://archibus.vodacom.co.za/Leasure-the-deed-will-the-clipt-Angely-ands-Banq?d=archibus.vodacom.co.za
https://archibus.vodacom.co.za/_Incapsula_Resource?SWJIYLWA=719d34d31c8e3a6e6fffd425f7e032f3&ns=14&cb=1544517188
https://archibus.vodacom.co.za/_Incapsula_Resource?SWJIYLWA=719d34d31c8e3a6e6fffd425f7e032f3&ns=7&cb=650421431
https://archibus.vodacom.co.za/_Incapsula_Resource?SWJIYLWA=719d34d31c8e3a6e6fffd425f7e032f3&ns=17&cb=316413804
https://archibus.vodacom.co.za/_Incapsula_Resource?SWJIYLWA=719d34d31c8e3a6e6fffd425f7e032f3&ns=19&cb=811508840
https://archibus.vodacom.co.za/_Incapsula_Resource?SWJIYLWA=719d34d31c8e3a6e6fffd425f7e032f3%22ns=19%22cb=811508840
https://archibus.vodacom.co.za/_Incapsula_Resource?SWJIYLWA=719d34d31c8e3a6e6fffd425f7e032f3&ns=52&cb=889049359
https://archibus.vodacom.co.za/_Incapsula_Resource?SWJIYLWA=719d34d31c8e3a6e6fffd425f7e032f3&ns=55&cb=1029309135
https://archibus.vodacom.co.za/_Incapsula_Resource?SWJIYLWA=719d34d31c8e3a6e6fffd425f7e032f3%22ns=36%22cb=1417430954
https://archibus.vodacom.co.za/_Incapsula_Resource?SWJIYLWA=719d34d31c8e3a6e6fffd425f7e032f3&ns=36&cb=1417430954
https://archibus.vodacom.co.za/_Incapsula_Resource?SWJIYLWA=719d34d31c8e3a6e6fffd425f7e032f3%22ns=35%22cb=1583299493
https://archibus.vodacom.co.za/_Incapsula_Resource?SWJIYLWA=719d34d31c8e3a6e6fffd425f7e032f3%22ns=46%22cb=1651641838

https://archibus.vodacom.co.za/_Incapsula_Resource?SWJIYLWA=719d34d31c8e3a6e6fffd425f7e032f3%22ns=62%22cb=20911158
https://archibus.vodacom.co.za/_Incapsula_Resource?SWJIYLWA=719d34d31c8e3a6e6fffd425f7e032f3%22ns=63%22cb=915183225
https://archibus.vodacom.co.za/_Incapsula_Resource?SWJIYLWA=719d34d31c8e3a6e6fffd425f7e032f3%22ns=73%22cb=290679225
https://archibus.vodacom.co.za/_Incapsula_Resource?SWJIYLWA=719d34d31c8e3a6e6fffd425f7e032f3&ns=35&cb=1583299493
https://archibus.vodacom.co.za/_Incapsula_Resource?SWJIYLWA=719d34d31c8e3a6e6fffd425f7e032f3&ns=61&cb=279001215
https://archibus.vodacom.co.za/_Incapsula_Resource?SWJIYLWA=719d34d31c8e3a6e6fffd425f7e032f3&ns=62&cb=20911158
https://archibus.vodacom.co.za/_Incapsula_Resource?SWJIYLWA=719d34d31c8e3a6e6fffd425f7e032f3&ns=46&cb=1651641838
https://archibus.vodacom.co.za/_Incapsula_Resource?SWJIYLWA=719d34d31c8e3a6e6fffd425f7e032f3&ns=63&cb=915183225
https://archibus.vodacom.co.za/_Incapsula_Resource?SWJIYLWA=719d34d31c8e3a6e6fffd425f7e032f3&ns=99&cb=631837770
https://archibus.vodacom.co.za/_Incapsula_Resource?SWJIYLWA=719d34d31c8e3a6e6fffd425f7e032f3&ns=73&cb=290679225
https://archibus.vodacom.co.za/_Incapsula_Resource?SWJIYLWA=719d34d31c8e3a6e6fffd425f7e032f3%22ns=83%22cb=723631670
https://archibus.vodacom.co.za/_Incapsula_Resource?SWJIYLWA=719d34d31c8e3a6e6fffd425f7e032f3&ns=83&cb=723631670
https://archibus.vodacom.co.za/_Incapsula_Resource?SWJIYLWA=719d34d31c8e3a6e6fffd425f7e032f3%22ns=84%22cb=1882006911
https://archibus.vodacom.co.za/_Incapsula_Resource?SWJIYLWA=719d34d31c8e3a6e6fffd425f7e032f3%22ns=94%22cb=2073905376
https://archibus.vodacom.co.za/_Incapsula_Resource?SWJIYLWA=719d34d31c8e3a6e6fffd425f7e032f3&ns=84&cb=1882006911
https://archibus.vodacom.co.za/_Incapsula_Resource?SWJIYLWA=719d34d31c8e3a6e6fffd425f7e032f3&ns=94&cb=2073905376

38116 SSL Server Information Retrieval (1)

38116 SSL Server Information Retrieval

archibus.vodacom.co.za:443/fpr/index.as

Finding #	10510234	**Severity**	Information Gathered - Level 1
Unique #	e22dd842-e31c-400c-85fd-f902f93fcb91		
Group	Scan Diagnostics		
CWE	-	**Detection Date**	11 Feb 2024 21:02 GMT+0200
OWASP	-		
WASC	-		

Details

Threat

The following is a list of supported SSL ciphers.

Note: If a cipher is included in this list it means that it was possible to establish a SSL connection using that cipher. There are some web servers setups that allow connections to be established using a LOW grade cipher, only to provide a web page stating that the URL is accessible only through a non-LOW grade cipher. In this case even though LOW grade cipher will be listed here QID 38140 will not be reported.

Impact

N/A

Solution

N/A

SSL Data

Flags	-
Protocol	tcp
Virtual Host	45.223.138.96
IP	45.223.138.96
Port	443
Result	#table cols="6" CIPHER KEY-EXCHANGE AUTHENTICATION MAC ENCRYPTION(KEY-STRENGTH) GRADE SSLv2_PROTOCOL_IS_DISABLED _ _ _ _ _ SSLv3_PROTOCOL_IS_DISABLED _ _ _ _ _ TLSv1_PROTOCOL_IS_DISABLED _ _ _ _ _ TLSv1.1_PROTOCOL_IS_DISABLED _ _ _ _ _ TLSv1.2_PROTOCOL_IS_ENABLED _ _ _ _ _ TLSv1.2 COMPRESSION_METHOD None _ _ _ AES128-SHA RSA RSA SHA1 AES(128) MEDIUM AES256-SH RSA RSA SHA1 AES(256) HIGH CAMELLIA128-SHA RSA RSA SHA1 Camellia(128) MEDIUM CAMELLIA256-SHA RSA RSA SHA1 Camellia(256) HIGH AES1 GCM-SHA256 RSA RSA AEAD AESGCM(128) MEDIUM AES256-GCM-SHA384 RSA RSA AEAD AESGCM(256) HIGH ECDHE-RSA-AES128-SHA ECDH RSA SHA1 AES(128) MEDIUM ECDHE-RSA-AES256-SHA ECDH RSA SHA1 AES(256) HIGH ECDHE-RSA-AES128-SHA256 ECDH RSA SHA256 AES(128) MEDI ECDHE-RSA-AES256-SHA384 ECDH RSA SHA384 AES(256) HIGH ECDHE-RSA-AES128-GCM-SHA256 ECDH RSA AEAD AESGCM(128) MEDIUM ECDHE RSA-AES256-GCM-SHA384 ECDH RSA AEAD AESGCM(256) HIGH ECDHE-RSA-CHACHA20-POLY1305 ECDH RSA AEAD CHACHA20/POLY1305(256) HI AES128-SHA256 RSA RSA SHA256 AES(128) MEDIUM AES256-SHA256 RSA RSA SHA256 AES(256) HIGH TLSv1.3_PROTOCOL_IS_ENABLED _ _ _ _ _

TLS13-AES-128-GCM-SHA256 N/A N/A AEAD AESGCM(128) MEDIUM TLS13-AES-256-GCM-SHA384 N/A N/A AEAD AESGCM(256) HIGH TLS13-CHACHA2
POLY1305-SHA256 N/A N/A AEAD CHACHA20/POLY1305(256) HIGH

Info List

Info #1

Ciphers

Name	Auth	Encryption	Grade	Key Exchange	Mac	Protocol
TLS13-AES-128-GCM-SHA256	N/A	AESGCM(128)	MEDIUM	N/A	AEAD	TLSv1.3
TLS13-AES-128-GCM-SHA256	N/A	AESGCM(256)	HIGH	N/A	AEAD	TLSv1.3
TLS13-AES-128-GCM-SHA256	N/A	CHACHA20/POLY1305(256)	HIGH	N/A	AEAD	TLSv1.3

38291 SSL Session Caching Information (1)

38291 SSL Session Caching Information *archibus.vodacom.co.za:443/fpr/index.as*

Finding #	10510228	**Severity**	Information Gathered - Level 1
Unique #	586f8139-a63c-44b3-bfaa-a4b78f7e6672		
Group	Scan Diagnostics		
CWE	-	**Detection Date**	11 Feb 2024 21:02 GMT+0200
OWASP	-		
WASC	-		

Details

Threat

SSL session is a collection of security parameters that are negotiated by the SSL client and server for each SSL connection. SSL session caching is targeted to reduce the overhead of negotiations in recurring SSL connections. SSL sessions can be reused to resume an earlier connection or to establish multiple simultaneous connections. The client suggests an SSL session to be reused by identifying the session with a Session-ID during SSL handshake. If the server finds it appropriate to reuse the session, then they both proceed to secure communication with already known security parameters.

This test determines if SSL session caching is enabled on the host.

Impact

SSL session caching is part of the SSL and TLS protocols and is not a security threat. The result of this test is for informational purposes only.

Solution

N/A

SSL Data

Flags	-
Protocol	tcp
Virtual Host	45.223.138.96
IP	45.223.138.96
	443

Port	
Result	TLSv1.2 session caching is enabled on the target. TLSv1.3 session caching is enabled on the target.

Info List

Info #1

38597 Secure Sockets Layer/Transport Layer Security (SSL/TLS) Invalid Protocol Version Tolerance (1)

38597 Secure Sockets Layer/Transport Layer Security (SSL/TLS) Invalid Protocol Version Tolerance

archibus.vodacom.co.za:443/fpr/index.as

Finding #	10510233	**Severity**	Information Gathered - Level 1
Unique #	19d07f36-71d2-443f-a103-6fb511475ef7		
Group	Scan Diagnostics		
CWE	-	**Detection Date**	11 Feb 2024 21:02 GMT+0200
OWASP	-		
WASC	-		

Details

Threat

SSL/TLS protocols have different version that can be supported by both the client and the server. This test attempts to send invalid protocol versions to the target in order to find out what is the target's behavior. The results section contains a table that indicates what was the target's response to each of our tests.

Impact

N/A

Solution

N/A

SSL Data

Flags	-
Protocol	tcp
Virtual Host	45.223.138.96
IP	45.223.138.96
Port	443
Result	#table cols=2 my_version target_version 0304 0303 0399 0303 0400 0303 0499 0303

Info List

Info #1

38600 SSL Certificate will expire within next six months (1)

38600 SSL Certificate will expire within next six months

archibus.vodacom.co.za:443/fpr/index.as

Finding #	10510227	**Severity**	Information Gathered - Level 1

Unique #	4951108d-0fff-450f-a3db-43611b3187bb		
Group	Scan Diagnostics		
CWE	-	**Detection Date**	11 Feb 2024 21:02 GMT+0200
OWASP	-		
WASC	-		

Details

Threat
Certificates are used for authentication purposes in different protocols such as SSL/TLS. Each certificate has a validity period outside of which it is supposed to be considered invalid. This QID is reported to inform that a certificate will expire within next six months. The advance notice can be helpful since obtaining a certificate can take some time.

Impact
Expired certificates can cause connection disruptions or compromise the integrity and privacy of the connections being protected by the certificates.

Solution
Contact the certificate authority that signed your certificate to arrange for a renewal.

SSL Data

Flags	-
Protocol	tcp
Virtual Host	45.223.138.96
IP	45.223.138.96
Port	443
Result	Certificate #0 CN=imperva.com The certificate will expire within six months: Jul 16 13:49:41 2024 GMT

Info List

Info #1

Certificate Fingerprint:5838E53F3C592C3FE144A59A3FF1EB4125C036D90CAEA8406E97249764E16408

38704 Secure Sockets Layer/Transport Layer Security (SSL/TLS) Key Exchange Methods (1)

38704 Secure Sockets Layer/Transport Layer Security (SSL/TLS) Key Exchange Methods *archibus.vodacom.co.za:443/fpr/index.as*

Finding #	10510235	**Severity**	Information Gathered - Level 1
Unique #	6869f2c0-d622-40e4-bcac-a5ff7f1e94f8		
Group	Scan Diagnostics		
CWE	-	**Detection Date**	11 Feb 2024 21:02 GMT+0200
OWASP	-		
WASC	-		

Details

Threat
The following is a list of SSL/TLS key exchange methods supported by the server, along with their respective key sizes, strengths and ciphers.

Impact

N/A

Solution
N/A

SSL Data

Flags	-
Protocol	tcp
Virtual Host	45.223.138.96
IP	45.223.138.96
Port	443
Result	#table cols="6" NAME GROUP KEY-SIZE FORWARD-SECRET CLASSICAL-STRENGTH QUANTUM-STRENGTH TLSv1.2 _ _ _ _ _ RSA _ 2048 no 110 low ECDHE x25519 256 yes 128 low ECDHE secp256r1 256 yes 128 low ECDHE x448 448 yes 224 low ECDHE secp521r1 521 yes 260 low ECDHE secp384r1 384 yes 192 low TLSv1.3 _ _ _ _ _ ECDHE x25519 256 yes 128 low ECDHE secp256r1 256 yes 128 low ECDHE x448 448 yes 224 low ECDHE secp521r1 521 yes low ECDHE secp384r1 384 yes 192 low

Info List

Info #1

Kexs

Kex	Group	Protocol	Key Size		Classical	Quantum
RSA		TLSv1.2	2048	no	110	low
ECDHE		TLSv1.2	256	yes	128	low
ECDHE		TLSv1.2	256	yes	128	low
ECDHE		TLSv1.2	448	yes	224	low
ECDHE		TLSv1.2	521	yes	260	low
ECDHE		TLSv1.2	384	yes	192	low
ECDHE		TLSv1.3	256	yes	128	low
ECDHE		TLSv1.3	256	yes	128	low
ECDHE		TLSv1.3	448	yes	224	low
ECDHE		TLSv1.3	521	yes	260	low
ECDHE		TLSv1.3	384	yes	192	low

38706 Secure Sockets Layer/Transport Layer Security (SSL/TLS) Protocol Properties (1)

38706 Secure Sockets Layer/Transport Layer Security (SSL/TLS) Protocol Properties *archibus.vodacom.co.za:443/fpr/index.as*

Finding #	10510236	**Severity**	Information Gathered - Level 1
Unique #	76a533a0-dd7a-42b6-af70-cd455d871756		
Group	Scan Diagnostics		
CWE	-	**Detection Date**	11 Feb 2024 21:02 GMT+0200
OWASP	-		
WASC	-		

Details

Threat
The following is a list of detected SSL/TLS protocol properties.

Impact
Items include:
- Extended Master Secret: indicates whether the extended_master_secret extension is supported or required by the server. This extension enhances security and is recommended. Applicable to TLSv1, TLSv1.1, TLSv1.2, DTLSv1, DTLSv1.2
- Encrypt Then MAC: indicates whether the encrypt_then_mac extension is supported or required by the server. This extension enhances the security of non-AEAD ciphers and is recommended. Applicable to TLSv1, TLSv1.1, TLSv1.2, DTLSv1, DTLSv1.2
- Heartbeat: indicates whether the heartbeat extension is supported. It is not recommended to enable this, except for DTLS. Applicable to TLSv1, TLSv1.1, TLSv1.2, TLSv1.3, DTLSv1, DTLSv1.2
- Truncated HMAC: indicates whether the truncated_hmac extension is supported. This can degrade security and is not recommended. Applicable to TLSv1, TLSv1.1, TLSv1.2, DTLSv1, DTLSv1.2
- Cipher priority: indicates whether client, server or both determine the priority of ciphers. Having the server determine the priority is recommended. Applicable to SSLv3, TLSv1, TLSv1.1, TLSv1.2, TLSv1.3, DTLSv1, DTLSv1.2

Solution
N/A

SSL Data

Flags	-
Protocol	tcp
Virtual Host	45.223.138.96
IP	45.223.138.96
Port	443
Result	#table cols="2" NAME STATUS TLSv1.2 _ Extended_Master_Secret yes Encrypt_Then_MAC yes Heartbeat no Truncated_HMAC no Cipher_priority_controlled_server OCSP_stapling no SCT_extension no TLSv1.3 _ Heartbeat no Cipher_priority_controlled_by server OCSP_stapling no SCT_extension no

Info List

Info #1

Props

Name	Value	Protocol
Extended Master Secret	yes	TLSv1.2
Encrypt Then MAC	yes	TLSv1.2
Heartbeat	no	TLSv1.2
Truncated HMAC	no	TLSv1.2
Cipher priority controlled by	server	TLSv1.2
OCSP stapling	no	TLSv1.2
SCT extension	no	TLSv1.2
Heartbeat	no	TLSv1.3
Cipher priority controlled by	server	TLSv1.3
OCSP stapling	no	TLSv1.3
SCT extension	no	TLSv1.3

38717 Secure Sockets Layer (SSL) Certificate Online Certificate Status Protocol (OCSP) Information (1)

38717 Secure Sockets Layer (SSL) Certificate Online Certificate Status Protocol (OCSP) Information

archibus.vodacom.co.za:443/fpr/index.as

Finding #	10510229	**Severity**	Information Gathered - Level 1
Unique #	fd47b632-f3e2-4d60-a5f1-2946ec063160		
Group	Scan Diagnostics		
CWE	-	**Detection Date**	11 Feb 2024 21:02 GMT+0200
OWASP	-		
WASC	-		

Details

Threat

OCSP (Online Certificate Status Protocol) is a protocol to determine the status of an SSL certificate, specifically whether a certificate has been revoked by the issuing certificate authority. SSL servers can provide the OCSP status of their certificate as part of the SSL/TLS handshake. This information is referred to as "Status Request" or "OCSP Stapling".

Impact

N/A

Solution

N/A

SSL Data

Flags	-
Protocol	tcp
Virtual Host	45.223.138.96
IP	45.223.138.96
Port	443
Result	Certificate #0 CN=archibus.vodacom.co.za,O=Vodafone_Group_Services_Limited,L=Newbury,C=GB OCSP status: good

Info List

Info #1

Certificate Fingerprint:0240E35B84FE2BCC96395D0CE97B03D511E35FC83F24034E9B73A3E054FA3A32

38718 Secure Sockets Layer (SSL) Certificate Transparency Information (1)

38718 Secure Sockets Layer (SSL) Certificate Transparency Information *archibus.vodacom.co.za:443/fpr/index.as*

Finding #	10510230	**Severity**	Information Gathered - Level 1
Unique #	481980a3-4e77-4196-b4a3-d532299fdb48		
Group	Scan Diagnostics		
CWE	-	**Detection Date**	11 Feb 2024 21:02 GMT+0200
OWASP	-		
WASC	-		

Details

Threat

SSL Certificate Transparency is an industry effort to improve visibility into the process of how certificate authorities issue certificates. It is designed to allow the owners of domain names to find all certificates that have been issued for their domains, and which certificate authorities have issued them. This is done by requiring certificate authorities to publish all issued certificates in public logs. TLS servers can then provide cryptographic evidence to TLS clients that the server certificate has been registered in public logs, thus providing some degree of confidence that the certificate is legitimate. Such cryptographic evidence is referred to as an "SCT Log Proof".

The information below lists all validated SCT Log Proofs for server certificates along with information about the public log, where available.

Impact

N/A

Solution

N/A

SSL Data

Flags	-
Protocol	tcp
Virtual Host	45.223.138.96
IP	45.223.138.96
Port	443
Result	#table cols="6" Source Validated Name URL ID Time Certificate_#0 _ CN=archibus.vodacom.co.za,O=Vodafone_Group_Services_Limited,L=Newbury,C=GB _ _

Certificate no (unknown) (unknown) eecdd064d5db1acec55cb79db4cd13a23287467cbcecdec351485946711fb59b Thu_01_Jan_1970_12:00:00_AM_GMT Certificate no (unknown) (unknown) 48b0e36bdaa647340fe56a02fa9d30eb1c5201cb56dd2c81d9bbbfab39d88473 Thu_01_Jan_1970_12:00:00_AM_GMT Certificate no (unknown) (unknown) dab6bf6b3fb5b6229f9bc2bb5c6be87091716cbb51848534bda43d3048d7fbab Thu_01_Jan_1970_12:00:00_AM_GMT Certificate_#0 _ CN=imperva.com _ _ _ Certificate no (unknown) (unknown) 76ff883f0ab6fb9551c261ccf587ba34b4a4cdbb29dc68420a9fe6674c5a3a74 Thu_01_Jan_1970_12:00:00_AM_GMT Certificate no (unknown) (unknown) 3b5377753e2db9804e8b305b06fe403b67d84fc3f4c7bd000d2d726fe1fad417 Thu_01_Jan_1970_12:00:00_AM_GMT Certificate no (unknown) (unknown) 48b0e36bdaa647340fe56a02fa9d30eb1c5201cb56dd2c81d9bbbfab39d88473 Thu_01_Jan_1970_12:00:00_AM_GMT

Info List

Info #1

Certificate Fingerprint:5838E53F3C592C3FE144A59A3FF1EB4125C036D90CAEA8406E97249764E16408

42350 TLS Secure Renegotiation Extension Support Information (1)

42350 TLS Secure Renegotiation Extension Support Information

archibus.vodacom.co.za:443/fpr/index.as

Finding #	10510232	**Severity**	Information Gathered - Level 1
Unique #	21a4fa31-8193-49a1-8275-c8893ceb39b3		
Group	Scan Diagnostics		
CWE	-	**Detection Date**	11 Feb 2024 21:02 GMT+0200
OWASP	-		
WASC	-		

Details

Threat

Secure Socket Layer (SSL) and Transport Layer Security (TLS) renegotiation are vulnerable to an attack in which the attacker forms a TLS connection with the target server, injects content of his choice, and then splices in a new TLS connection from a client. The server treats the client's initial TLS handshake as a renegotiation and thus believes that the initial data transmitted by the attacker is from the same entity as the subsequent client data. TLS protocol was extended to cryptographically tierenegotiations to the TLS connections they are being performed over. This is referred to as TLS secure renegotiation extension. This detection determines whether the TLS secure renegotiation extension is supported by the server or not.

Impact

N/A

Solution

N/A

SSL Data

Flags	-
Protocol	tcp
Virtual Host	45.223.138.96
IP	45.223.138.96
Port	443
Result	TLS Secure Renegotiation Extension Status: supported.

Info List

Info #1

WAS Web Application Report

45038 Host Scan Time - Scanner (1)

45038 Host Scan Time - Scanner

archibus.vodacom.co.za:443/fpr/index.as

Finding #	10510211	**Severity**	Information Gathered - Level 1
Unique #	402defad-8ff7-4d02-952a-1442b5787d3a		
Group	Scan Diagnostics		
CWE	-	**Detection Date**	11 Feb 2024 21:02 GMT+0200
OWASP	-		
WASC	-		

Details

Threat

The Host Scan Time is the period of time it takes the scanning engine to perform the vulnerability assessment of a single target host. The Host Scan Time for this host is reported in the Result section below.

The Host Scan Time does not have a direct correlation to the Duration time as displayed in the Report Summary section of a scan results report. The Duration is the period of time it takes the service to perform a scan task. The Duration includes the time it takes the service to scan all hosts, which may involve parallel scanning. It also includes the time it takes for a scanner appliance to pick up the scan task and transfer the results back to the service's Secure Operating Center. Further, when a scan task is distributed across multiple scanners, the Duration includes the time it takes to perform parallel host scanning on all scanners.

Impact

N/A

Solution

N/A

SSL Data

Flags	-
Protocol	-
Virtual Host	archibus.vodacom.co.za
IP	45.223.138.96
Port	-
Result	Scan duration: 5412 seconds Start time: Sun Feb 11 19:02:08 UTC 2024 End time: Sun Feb 11 20:32:20 UTC 2024

Info List

Info #1

6 DNS Host Name (1)

6 DNS Host Name

archibus.vodacom.co.za:443/fpr/index.as

Finding #	10510225	**Severity**	Information Gathered - Level 1
Unique #	5d9824b8-2dd0-4877-b6f7-c2788f9e035c		
Group	Scan Diagnostics		
CWE	-	**Detection Date**	11 Feb 2024 21:02 GMT+0200
OWASP	-		
WASC	-		

Details

Threat
The fully qualified domain name of this host, if it was obtained from a DNS server, is displayed in the RESULT section.

Impact
N/A

Solution
N/A

SSL Data

Flags	-
Protocol	-
Virtual Host	45.223.138.96
IP	45.223.138.96
Port	-
Result	#table IP_address Host_name 45.223.138.96 No_registered_hostname

Info List

Info #1

86002 SSL Certificate - Information (1)

86002 SSL Certificate - Information *archibus.vodacom.co.za:443/fpr/index.as*

Finding #	10510226	**Severity**	Information Gathered - Level 1
Unique #	ff2a844d-4dee-41d5-b061-a326d36a93b4		
Group	Scan Diagnostics		
CWE	-	**Detection Date**	11 Feb 2024 21:02 GMT+0200
OWASP	-		
WASC	-		

Details

Threat
SSL certificate information is provided in the Results section.

Impact
N/A

Solution
N/A

SSL Data

Flags	-

WAS Web Application Report

Protocol	tcp
Virtual Host	45.223.138.96
IP	45.223.138.96
Port	443
Result	#table cols="2" NAME VALUE (0)CERTIFICATE_0 _ (0)Version 3_(0x2) (0)Serial_Number _05:c6:21:a0:8b:cb:9d:a5:a9:50:27:34:56:03:00:0f_ (0)Signature_Algorithm sha256WithRSAEncryption (0)ISSUER_NAME _ countryName US _organizationName DigiCert_Inc _commonName DigiCert_SHA2_Secure_Server_CA (0)SUBJECT_NAME _ countryName GB _localityName Newbury _organizationName Vodafone_Group_Services_Limited _commonName archibus.vodacom.co.za (0)Valid_From Aug_11_00:00:00_2023_GMT (0)Valid_Till Aug_13_23:59:59_2024_GMT (0)Public_Key_Algorithm rsaEncryption (0)RSA_Public_Key (2048_bit) (0) _RSA_Public-Key:_(2048_bit) (0) _Modulus: (0) _00:95:50:81:28:a9:f1:89:02:18:87:b2:cb:e9:6f: (0) _6d:73:ee:e6 92:08:28:0b:71:fc:d7:01:34:86: (0) _43:c0:9c:74:c4:23:a9:cc:ef:d1:8d:61:25:27:3d: (0) _9f:f0:8b:65:be:57:1e:76:2e:e0:75:ca:9b:b1:8e: (0) _11:b5:5c:8b: 58:07:77:d1:15:e3:fc:f5:cc:31:6a: (0) _9c:01:42:f9:7a:02:61:6d:fe:33:2e:1f:85:9a:d3: (0) _e0:b5:89:ff:0b:38:1d:4f:9f:ee:6e:00:46:37:e1: (0) _bb:91:9d:cf: 76:14:43:c4:e2:33:21:f4:b4:5d:23: (0) _e7:86:d9:73:54:7c:7e:d4:5e:67:63:e1:22:d6:6a: (0) _2f:11:28:e3:0f:68:ef:1f:47:78:e4:98:55:af:af: (0) _54:08:91:ab:be: 24:21:78:59:f0:01:e6:70:b6:da: (0) _18:ae:48:65:e3:e8:2f:d1:bf:66:ca:1c:df:ce:01: (0) _14:51:20:51:5a:62:e4:83:c4:45:67:2a:e2:9d:a2: (0) _d8:1d:89:89:fd: 47:14:db:e6:8d:eb:53:55:89:5e: (0) _c0:70:b8:95:1a:7f:c7:00:b8:7a:3c:a9:be:03:cc: (0) _d8:21:8e:17:16:01:7e:9d:59:20:ef:aa:7d:8e:c4: (0) _3f:18:83:93:4f:ff:68:6e: 57:ae:ec:b7:8e:85:67: (0) _d9:3d (0) _Exponent:_65537_(0x10001) (0)X509v3_EXTENSIONS _ (0)X509v3_Authority_Key_Identifier _keyid:0F:80:61:1C: 82:31:61:D5:2F:28:E7:8D:46:38:B4:2C:E1:C6:D9:E2 (0)X509v3_Subject_Key_Identifier _57:7C:F8:D6:FD:53:52:92:12:99:03:79:B7:5D:F8:9E:18:CB:46:91 (0)X509v3_Subject_Alternative_Name _DNS:archibus.vodacom.co.za,_DNS:archibustest.vodacom.co.za,_DNS:archibusdev.vodacom.co.za (0)X509v3_Key_Usa critical (0) _Digital_Signature,_Key_Encipherment (0)X509v3_Extended_Key_Usage _TLS_Web_Server_Authentication,_TLS_Web_Client_Authentication (0)X509v3_CRL_Distribution_Points (0) _Full_Name: (0) _URI:http://crl3.digicert.com/DigicertSHA2SecureServerCA-1.crl (0) (0) _Full_Name: (0) _URI:http:// crl4.digicert.com/DigicertSHA2SecureServerCA-1.crl (0)X509v3_Certificate_Policies _Policy:_2.23.140.1.2.2 (0) _CPS:_http://www.digicert.com/CPS (0)Authority_Information_Access _OCSP_-_URI:http://ocsp.digicert.com (0) _CA_Issuers_-_URI:http://cacerts.digicert.com/DigiCertSHA2SecureServerCA-2.crt (0)X509v3_Basic_Constraints _CA:FALSE (0)CT_Precertificate_SCTs _Signed_Certificate_Timestamp: (0) _Version_:_v1_(0x0) (0) _Log_ID_:_EE:CD:D0:64:D5: 1A:CE:C5:5C:B7:9D:B4:CD:13:A2: (0) _32:87:46:7C:BC:EC:DE:C3:51:48:59:46:71:1F:B5:9B (0) _Timestamp_:_Aug_11_07:53:07.437_2023_GMT (0) _Extensions:_none (0) _Signature_:_ecdsa-with-SHA256 (0) _30:44:02:20:1C:66:C4:F7:06:8A:11:30:10:90:17:5F: (0) _2E:D9:7B:96:1F:80:16:0A:7E:39:A7:42:61: 24:79: (0) _60:64:13:59:02:20:7F:9C:0B:46:69:F1:D1:52:D5:DB: (0) _C2:90:5E:8D:07:36:59:42:44:A5:10:21:B5:D5:E2:2A: (0) _12:2B:BE:A3:79:F6 (0) _Signed_Certificate_Timestamp: (0) _Version_:_v1_(0x0) (0) _Log_ID_:_48:B0:E3:6B:DA:A6:47:34:0F:E5:6A:02:FA:9D:30:EB: (0) _1C:52:01:CB:56:DD:2C: 81:D9:BB:BF:AB:39:D8:84:73 (0) _Timestamp_:_Aug_11_07:53:07.439_2023_GMT (0) _Extensions:_none (0) _Signature_:_ecdsa-with-SHA256 (0) _30:45:02:20:70:D6:33:72:DD:4A:69:7A:A9:34:BF:72: (0) _71:E0:A8:79:E1:49:E0:B0:2A:45:E7:6F:FB:55:36:CA: (0) _D0:D2:17:8C:02:21:00:AB:FD:F7:70:AC:FF:I 7B:90: (0) _F5:3A:89:BD:F8:C1:4C:D5:1E:AD:03:36:F8:86:4B:26: (0) _15:CF:78:CD:28:BF:FB (0) _Signed_Certificate_Timestamp: (0) _Version_:_v1_(0x0) (0) _Log_ID_:_DA:B6:BF:6B:3F:B5:B6:22:9F:9B:C2:BB:5C:6B:E8:70: (0) _91:71:6C:BB:51:84:85:34:BD:A4:3D:30:48:D7:FB:AB (0) _Timestamp_:_Aug_11_07:53:07.365_2023_GMT (0) _Extensions:_none (0) _Signature_:_ecdsa-with-SHA256 (0) _30:45:02:21:00:82:73:A3:F7:55:A7:B7:B1:D7:19:6F: (0) _1A:B5:29:0A:86:B5:F9:BE:C1:C1:17:27:2C:EB:E0:2B: (0) _DE:71:4D:19:B3:02:20:5D:91:77:0D: 14:C5:43:6F:CB: (0) _FF:D3:70:A7:F6:65:18:08:E8:C6:5F:23:9B:3D:C3:84: (0) _59:64:8E:A0:2B:97:64 (0)Signature (256_octets) (0) ae: 83:b0:2d:c3:df:a7:d2:8a:b0:08:99:9e:28:c8:79 (0) 62:b8:3d:77:de:97:d6:b9:b5:1a:eb:90:a4:64:75:41 (0) 35:95:08:02:61:c7:8c:0c:8a:dd:6b:9b:81:69:9e:f0 (0) b0:df: 03:27:f1:6c:85:c1:04:86:f7:4d:2d:3a:07:f6 (0) 93:5c:f3:aa:66:51:ed:55:48:8e:50:e5:5f:f0:1c:03 (0) c2:83:ff:d2:c5:69:e0:dc:48:28:b3:c8:91:55:4b:a0 (0) 8a:fc:9f:8b: 26:9d:ce:3b:13:c0:d4:9a:a2:bf:a9:6f (0) d2:e7:77:5a:ef:5f:6f:e0:f5:bf:f6:56:58:41:98:ae (0) 0e:39:cf:11:32:16:67:0e:00:b5:ed:9b:54:02:e1:b9 (0) cf:0b: 38:81:13:b4:08:e6:d2:c0:3d:bc:7f:8a:5e:1d (0) f1:55:38:97:04:07:db:62:44:ba:15:df:50:3d:15:06 (0) b7:e5:c4:47:8f:55:a7:98:13:86:08:3c:9d:f9:d9:3a (0) 24:94:0f: 6b:a6:ae:87:3f:1d:71:c3:3f:90:75:c0:96 (0) 2d:dc:90:ee:e6:d3:30:47:68:56:26:2b:d8:18:28:3e (0) c0:11:8c:65:cc:84:dd:b1:f0:24:42:df:eb:d4:7f:b8 (0) 57:a9:21:f1:70:22:f0:7d:c2:25:09:14:04:92:20:40 (1)CERTIFICATE_1 _ (1)Version 3_(0x2) (1)Serial_Number _02:74:2e:aa:17:ca:8e:21:c7:17:bb:1f:fc:fd:0c:a0_ (1)Signature_Algorithm sha256WithRSAEncryption (1)ISSUER_NAME _ countryName US _organizationName DigiCert_Inc _organizationalUnitName www.digicert.com _commonName DigiCert_Global_Root_CA (1)SUBJECT_NAME _ countryName US _organizationName DigiCert_Inc _commonName DigiCert_SHA2_Secure_Server_CA (1)Valid_From Sep_23_00:00:00_2020_GMT (1)Valid_Till Sep_22_23:59:59_2030_GMT (1)Public_Key_Algorithm rsaEncryption (1)RSA_Public_Key (2048_bit) (1) _RSA_Public-Key:_(2048_bit) (1) _Modulus: (1) _00:dc:ae:58:90:4d:c1:c4:30:15:90:35:5b:6e:3c: (1) _82:15:f5:2c 5c:bd:e3:db:ff:71:43:fa:64:25:80: (1) _d4:ee:18:a2:4d:f0:66:d0:0a:73:6e:11:98:36:17: (1) _64:af:37:9d:fd:fa:41:84:af:c7:af:8c:fe:1a:73: (1) _4d:cf: 33:97:90:a2:96:87:53:83:2b:b9:a6:75:48: (1) _2d:1d:56:37:7b:da:31:32:1a:d7:ac:ab:06:f4:aa: (1) _5d:4b:b7:47:46:dd:2a:93:c3:90:2e:79:80:80:ef: (1) _13:04:6a: 14:3b:b5:9b:92:be:c2:07:65:4e:fc:da: (1) _fc:ff:7a:ae:dc:5c:7e:55:31:0c:e8:39:07:a4:d7: (1) _be:2f:d3:0b:6a:d2:b1:df:5f:fe:57:74:53:3b:35: (1) _80:dd:ae:8e: 44:98:b3:9f:0e:d3:da:e0:d7:f4:6b: (1) _29:ab:44:a7:4b:58:84:6d:92:4b:81:c3:da:73:8b: (1) _12:97:48:90:04:45:75:1a:dd:37:31:97:92:e8:cd: (1) _54:0d:3b:e4:c1:3f: 39:5e:2e:b8:f3:5c:7e:10:8e: (1) _86:41:00:8d:45:66:47:b0:a1:65:ce:a0:aa:29:09: (1) _4e:f3:97:eb:e8:2e:ab:0f:72:a7:30:0e:fa:c7:f4: (1) _fd:14:77:c3:a4:5b: 28:57:c2:b3:f9:82:fd:b7:45: (1) _58:9b (1) _Exponent:_65537_(0x10001) (1)X509v3_EXTENSIONS _ (1)X509v3_Subject_Key_Identifier _0F:80:61:1C: 82:31:61:D5:2F:28:E7:8D:46:38:B4:2C:E1:C6:D9:E2 (1)X509v3_Authority_Key_Identifier _keyid:03:DE:50:35:56:D1:4C:BB:66:F0:A3:E2:1B:1B:C3:97:B2:3D:D1:5 (1)X509v3_Key_Usage critical (1) _Digital_Signature,_Certificate_Sign,_CRL_Sign (1)X509v3_Extended_Key_Usage _TLS_Web_Server_Authentication,_TLS_Web_Client_Authentication (1)X509v3_Basic_Constraints critical (1) _CA:TRUE,_pathlen:0 (1)Authority_Information_Access _OCSP_-_URI:http://ocsp.digicert.com (1) _CA_Issuers_-_URI:http://cacerts.digicert.com/DigiCertGlobalRootCA.crt (1)X509v3_CRL_Distribution_Points (1) _Full_Name: (1) _URI:http://crl3.digicert.com/DigiCertGlobalRootCA.crl (1) (1) _Full_Name: (1) _URI:http://crl4.digicert.cor DigiCertGlobalRootCA.crl (1)X509v3_Certificate_Policies _Policy:_2.23.140.1.1 (1) _Policy:_2.23.140.1.2.1 (1) _Policy:_2.23.140.1.2.2 (1) _Policy:_2.23.140.1.2.3 (1)Signature (256_octets) (1) 77:31:1f:08:97:d7:12:9b:63:d2:11:65:08:a6:f6:65 (1) b9:b8:fa:92:03:cb:a1:7e:e1:c8:0d:8c:3e:b4:1b:91 (1) be:02:08:5e:9f:59:71:7b: 11:fd:e0:c0:e3:8f:59:d7 (1) a0:52:a1:d0:4b:54:d2:48:96:48:ef:77:e9:29:06:cb (1) 43:10:a0:2f:3c:16:8e:2d:fe:1e:55:3c:ec:c3:98:ee (1) 18:0d:23:e8:07:f5:b3:2d:c4:ab 57:73:5a:f6:1b:53 (1) ba:fb:1f:fa:bd:8c:d3:51:51:20:47:5e:ef:7f:98:ab (1) 17:42:ca:85:5c:9f:22:37:34:45:76:f2:43:5e:00:9e (1) 22:83:ac:df:af:d1:e6:c7:13:17:e9:a4:69:64:4c:80 (1) 67:ea:b6:a4:7f:8f:7d:e1:51:fa:9e:97:67:ea:69:2e (1) b3:90:a4:1c:15:c8:ac:cb:4f:29:ec:7a:5c:5d:9f:8a (1) b8:d4:0c:bb:94:ee:d0:bc:cb:b5:a5:1e:08:cf:c4:41 (1) 03:0d:bd:06:c3:a0:f4:c8:37:55:4a:f1:bf:e5:79:42 (1) 35:ab:41:98:ef:fc:13:39:c3:bb:5b:eb:ef:63:7c:80 (1) 9c:c8:49:46:70:6b:a0:82:50:3e:d0:04:b6:ca:25:c5 (1) c1:05:55:5f:f2:7c:2f:57:d1:af:95:6f:ac:6d:79:6b (2)CERTIFICATE_2 _ (2)Version 3_(0x2) (2)Serial_Number _08:3b:e0:56:90:42:46:b1:a1:75:6a:c9:59:91:c7:4a_ (2)Signature_Algorithm sha1WithRSAEncryption (2)ISSUER_NAME _ countryName US _organizationName DigiCert_Inc _organizationalUnitName www.digicert.com _commonName DigiCert_Global_Root_CA (2)SUBJECT_NAME _ countryName US _organizationName DigiCert_Inc _organizationalUnitName www.digicert.com _commonName DigiCert_Global_Root_CA (2)Valid_From Nov_10_00:00:00_2006_GMT (2)Valid_Till Nov_10_00:00:00_2031_GMT (2)Public_Key_Algorithm rsaEncryption (2)RSA_Public_Key (2048_bit) (2) _RSA_Public-Key:_(2048_bit) (2) _Modulus: (2) _00:e2:3b:e1:11:72:de:a8:a4:d3:a3:57:aa:50:a2: (2) _8f:0b:77:90:c9:a2:a5:ee:12:ce:96:5b:01:09:20: (2) _cc:01:93:a7:4e:30:b7:53:f7:43:c4:69:00:57:9d: (2) _e2:8d 22:dd:87:06:40:00:81:09:ce:ce:1b:83:bf: (2) _df:cd:3b:71:46:e2:d6:66:c7:05:b3:76:27:16:8f: (2) _7b:9e:1e:95:7d:ee:b7:48:a3:08:da:d6:af:7a:0c: (2) _39:06:65:7f:4a 5d:1f:bc:17:f8:ab:be:ee:28:d7: (2) _74:7f:7a:78:99:59:85:68:6e:5c:23:32:4b:bf:4e: (2) _c0:e8:5a:6d:e3:70:bf:77:10:bf:fc:01:f6:85:d9: (2) _a8:44:10:58:32:a9:75:18:d5:d1:a2:be:47:e2:27: (2) _6a:f4:9a:33:f8:49:08:60:8b:d4:5f:b4:3a:84:bf: (2) _a1:aa:4a:4c:7d:3e:cf:4f:5f:6c:76:5e:a0:4b:37: (2) _91:9e:dc 22:e6:6d:ce:14:1a:8e:6a:cb:fe:cd:b3: (2) _14:64:17:c7:5b:29:9e:32:bf:f2:ee:fa:d3:0b:42: (2) _d4:ab:b7:41:32:da:0c:d4:ef:f8:81:d5:bb:8d:58: (2) _3f:b5:1b:e8:49:28:a2:70:da:31:04:dd:f7:b2:16: (2) _f2:4c:0a:4e:07:a8:ed:4a:3d:5e:b5:7f:a3:90:c3: (2) _af:27 (2) _Exponent:_65537_(0x10001) (2)X509v3_EXTENSIONS _ (2)X509v3_Key_Usage critical (2) _Digital_Signature,_Certificate_Sign,_CRL_Sign (2)X509v3_Basic_Constraints critical (2) _CA:TRU (2)X509v3_Subject_Key_Identifier _03:DE:50:35:56:D1:4C:BB:66:F0:A3:E2:1B:1B:C3:97:B2:3D:D1:55 (2)X509v3_Authority_Key_Identifier _keyid:03:DE: 50:35:56:D1:4C:BB:66:F0:A3:E2:1B:1B:C3:97:B2:3D:D1:55 (2)Signature (256_octets) (2) cb:9c:37:aa:48:13:12:0a:fa:dd:44:9c:4f:52:b0:f4 (2) df:ae: 04:f5:79:79:08:a3:24:18:fc:4b:2b:84:c0:2d (2) b9:d5:c7:fe:f4:c1:1f:58:cb:b8:6d:9c:7a:74:e7:98 (2) 29:ab:11:b5:e3:70:a0:a1:cd:4c:88:99:93:8c:91:70 (2) e2:ab:0f:1c: 93:a9:ff:63:d5:e4:07:60:d3:a3:bf (2) 9d:5b:09:f1:d5:8e:e3:53:f4:8e:63:fa:3f:a7:db:b4 (2) 66:df:62:66:d6:d1:6e:41:8d:f2:2d:b5:ea:77:4a:9f (2) 9d:58:e2:2b: 59:c0:40:23:ed:2d:28:82:45:3e:79:54 (2) 92:26:98:e0:80:48:a8:37:ef:f0:d6:79:60:16:de:ac (2) e8:0e:cd:6e:ac:44:17:38:2f:49:da:e1:45:3e:2a:b9 (2) 36:53:cf:3a: 50:06:f7:2e:e8:c4:57:49:6c:61:21:18 (2) d5:04:ad:78:3c:2c:3a:80:6b:a7:eb:af:15:14:e9:d8 (2) 89:c1:b9:38:6c:e2:91:6c:8a:ff:64:b9:77:25:57:30 (2) c0:1b:

24:a3:e1:dc:e9:df:47:7c:b5:b4:24:08:05:30 (2) ec:2d:bd:0b:bf:45:bf:50:b9:a9:f3:eb:98:01:12:ad (2) c8:88:c6:98:34:5f:8d:0a:3c:c6:e9:d5:95:95:6d:de #table cols="2
NAME VALUE (0)CERTIFICATE_0 _ (0)Version 3_(0x2) (0)Serial_Number _01:8c:fc:40:a6:82:cc:44:37:35:84:76:9e:2f:e7:2a_ (0)Signature_Algorithm
sha256WithRSAEncryption (0)ISSUER_NAME _ countryName BE _organizationName GlobalSign_nv-sa _commonName
GlobalSign_Atlas_R3_DV_TLS_CA_2024_Q1 (0)SUBJECT_NAME _ commonName imperva.com (0)Valid_From Jan_18_13:49:41_2024_GMT (0)Valid_Till
Jul_16_13:49:41_2024_GMT (0)Public_Key_Algorithm rsaEncryption (0)RSA_Public_Key (2048_bit) (0) _RSA_Public-Key:_(2048_bit) (0) _Modulus: (0)
_00:b4:45:53:af:8c:d2:ca:21:2c:0c:a2:ea:0d:53: (0) _f4:17:ae:ad:ab:28:95:7d:5f:31:74:3d:7d:1a:3f: (0) _d6:c8:3c:cc:bc:b0:bb:ce:42:2f:cb:76:73:fb:3b: (0) _ef:44:8
4a:30:61:c0:c1:7f:6e:f9:03:e2:c8: (0) _0c:98:5a:b0:c4:00:47:93:dc:84:89:e4:50:91:09: (0) _39:a8:45:f1:97:61:4d:82:a4:4c:ce:d9:71:fd:01: (0) _e0:9f:
57:fa:c1:5a:da:ee:a1:6a:94:86:bd:20:93: (0) _e5:14:ed:60:6d:3e:db:a5:c2:cc:85:24:64:16:62: (0) _88:34:c1:12:7f:bc:f7:8c:8e:76:32:30:9d:dd:79: (0)
_7b:b0:4a:f6:38:f5:bc:ef:a8:99:cc:c3:15:ca:a9: (0) _0a:db:e1:64:71:fc:13:0b:6c:e8:4a:63:8e:f9:a8: (0) _3c:bb:ed:78:70:ab:3c:bd:27:e7:38:61:8a:2a:3b: (0)
_51:67:00:70:99:88:af:4b:ae:35:17:e0:83:02:34: (0) _f5:13:b1:96:16:41:50:60:99:41:39:fb:01:b0:4f: (0) _71:ad:20:53:dd:ad:8b:1d:aa:eb:06:40:bc:9c:08: (0) _9d:8
0d:bb:33:6d:f4:91:a7:80:0f:4e:c9:29:6b: (0) _0d:34:6a:14:a8:62:72:bd:a9:92:29:c5:29:ec:d8: (0) _1b:47 (0) _Exponent:_65537_(0x10001) (0)X509v3_EXTENSIO
_ (0)X509v3_Subject_Alternative_Name
_DNS:lending.vodacom.co.za,_DNS:hyperbook.vodacom.co.za,_DNS:journalist.vodacom.co.za,_DNS:de.c3dcrm.ppiam.vodacom.co.za,_DNS:nc.m2.ppret.voda
pwmicros.vodacom.co.za,_DNS:m2d.ret.vodacom.co.za,_DNS:kw3118.vod (0)
acom.co.za,_DNS:ciims.vodacom.co.za,_DNS:ifsfsmqa.vodacom.co.za,_DNS:cdn.mobucks.vodacom.co.za,_DNS:apix.vodacom.co.za,_DNS:nc.m2d.iam.vodac
ubuntu.vodacom.co.ls,_DNS:business.vodacom.co.za,_DNS:cc.m2d.ret.vodacom.co.za,_DNS:cc.m2.ppret.vodacom.co.za,_DNS:mobucks.sso. (0)
vodacom.co.za,_DNS:next.vodacom.co.za,_DNS:ifsfsm.vodacom.co.za,_DNS:cognosqa.sso.vodacom.co.za,_DNS:fr.m2.iam.vodacom.co.za,_DNS:nc.m2.iam.v
crm1.vodacom.co.za,_DNS:aplus-
dev.vodacom.co.za,_DNS:sorteos.mivodafoneapp.es,_DNS:login.ret.vodacom.co.za,_DNS:fr.m2d.ppret.vodacom.co.za,_DNS:etomrsso.vodacom.co.za,_DNS:fr
(0) nts.vodacom.co.za,_DNS:de.m2d.ppret.vodacom.co.za,_DNS:lendingdev.vodacom.co.za,_DNS:c3d-
crm.vodacom.co.za,_DNS:engageplatform.vodacom.co.za,_DNS:archibus.vodacom.co.za,_DNS:dwp.vodacom.co.za,_DNS:mobucks.ppent.vodacom.co.za,_DN
(0) _DNS:hcsadminapi.voicespend.vodacom.co.za,_DNS:m2.ppret.vodacom.co.za,_DNS:aplus-
qa.vodacom.co.za,_DNS:login.ent.vodacom.co.za,_DNS:de.c3dcrm.iam.vodacom.co.za,_DNS:public.tobicloud-
dev.vodafone.it,_DNS:consent.ppsso.vodacom.co.za,_DNS:*.to-
zi.com,_DNS:cc.m2d.iam.vodacom.co.za,_DNS:cc.m2.ppiam.vodacom.co.za,_DNS:login.thanos.co.za,_DNS:bcmapp.vodacom.co.za,_DNS:irsp.iam.vodacom.c
zi.com,_DNS:lendingqa.vodacom.co.za (0)X509v3_Key_Usage critical (0) _Digital_Signature,_Key_Encipherment (0)X509v3_Extended_Key_Usage
_TLS_Web_Server_Authentication,_TLS_Web_Client_Authentication (0)X509v3_Subject_Key_Identifier _2D:75:CE:D0:C6:36:E7:0A:AA:
02:47:60:D3:D3:07:25:22:48:58:17 (0)X509v3_Certificate_Policies _Policy:_2.23.140.1.2.1 (0) _Policy:_1.3.6.1.4.1.4146.10.1.3 (0) _CPS:_https://
www.globalsign.com/repository/ (0)X509v3_Basic_Constraints critical (0) _CA:FALSE (0)Authority_Information_Access _OCSP_-_URI:http://ocsp.globalsign.com
gsatlasr3dvtlsca2024q1 (0) _CA_Issuers_-_URI:http://secure.globalsign.com/cacert/gsatlasr3dvtlsca2024q1.crt (0)X509v3_Authority_Key_Identifier _keyid:
66:C0:C7:A3:9A:CD:FE:F3:EA:CE:4B:53:0B:61:5E:AF:33:05:B3:E1 (0)X509v3_CRL_Distribution_Points (0) _Full_Name: (0) _URI:http://crl.globalsign.com/ca/
gsatlasr3dvtlsca2024q1.crl (0)CT_Precertificate_SCTs _Signed_Certificate_Timestamp: (0) _Version_:_v1_(0x0) (0) _Log_ID_:_76:FF:88:3F:0A:B6:FB:
95:51:C2:61:CC:F5:87:BA:34: (0) _B4:A4:CD:BB:29:DC:68:42:0A:9F:E6:67:4C:5A:3A:74 (0) _Timestamp_:_Jan_18_13:50:14.915_2024_GMT (0)
_Extensions:_none (0) _Signature_:_ecdsa-with-SHA256 (0) _30:45:02:20:2A:87:69:07:90:39:65:94:75:77:FF:D0: (0) _36:EF:3A:28:9F:5B:44:AD:9D:34:CC:7F:
70:D1:22:2D: (0) _1D:BB:0B:09:02:21:00:A1:47:3B:73:1C:9B:16:4F:E7: (0) _21:3D:DA:DE:02:27:B5:7E:5D:D8:76:30:7E:97:0B:76: (0) _1A:51:40:FC:60:E3:B5 (0
_Signed_Certificate_Timestamp: (0) _Version_:_v1_(0x0) (0) _Log_ID_:_3B:53:77:75:3E:2D:B9:80:4E:8B:30:5B:06:FE:40:3B: (0) _67:D8:4F:C3:F4:C7:BD:00:0
72:6F:E1:FA:D4:17 (0) _Timestamp_:_Jan_18_13:50:15.031_2024_GMT (0) _Extensions:_none (0) _Signature_:_ecdsa-with-SHA256 (0)
_30:45:02:20:08:14:0B:B5:56:12:65:11:C8:E1:F3:AC: (0) _E8:FF:94:C8:5E:A0:2D:F7:7E:7B:13:6F:CA:64:CE:0E: (0) _18:F2:49:2C:02:21:00:E6:E6:BB:AF:89:7E
02:33:44: (0) _19:4C:6A:22:98:CD:E1:61:36:C0:FA:58:92:BB:E8:32: (0) _1C:E2:2F:11:B1:D3:D4 (0) _Signed_Certificate_Timestamp: (0) _Version_:_v1_(0x0) (0
_Log_ID_:_48:B0:E3:6B:DA:A6:47:34:0F:E5:6A:02:FA:9D:30:EB: (0) _1C:52:01:CB:56:DD:2C:81:D9:BB:BF:AB:39:D8:84:73 (0)
Timestamp:_Jan_18_13:50:15.338_2024_GMT (0) _Extensions:_none (0) _Signature_:_ecdsa-with-SHA256 (0) _30:45:02:21:00:83:84:EC:EF:2B:
59:53:02:10:C9:3C: (0) _0E:99:97:D8:50:35:1C:E5:9B:7F:46:01:8C:44:B2:F9: (0) _23:3E:9D:DB:CB:02:20:47:02:FE:EC:BD:B4:D5:1D:49: (0) _FF:17:9F:
01:12:47:EA:AA:E0:A8:72:E8:21:49:43:6D: (0) _CC:9F:4C:C2:42:16:73 (0)Signature (256_octets) (0) 7a:c3:19:8f:f8:f8:52:33:00:a5:aa:ef:21:09:db:48 (0)
a0:d3:62:75:cc:48:c4:2d:ed:84:27:95:28:cd:30:d4 (0) 11:2a:65:8b:83:ea:21:d8:1b:d2:4f:01:10:35:01:dd (0) e8:65:c1:a4:4a:64:06:46:24:a6:65:45:38:f9:6c:3b (0)
85:11:80:65:84:40:97:16:25:bf:c0:26:75:6d:6c:4c (0) a2:0d:ea:d4:16:f1:be:72:3b:da:a7:50:43:7d:22:18 (0) 3f:43:88:2e:9b:dd:53:9e:8f:28:88:84:d6:d9:be:77 (0) 2d
66:d1:f1:25:7a:ba:00:40:2f:11:67:98:81:ab (0) 04:21:79:dd:b0:6b:c1:f1:b5:f1:7e:89:72:fc:55:39 (0) 7c:3e:53:2d:c5:d3:fb:e3:43:b7:ae:06:f3:98:1a:41 (0) 8d:
5d:e2:80:84:dc:a5:7d:92:5f:d1:e5:1a:d2:c8:50 (0) 32:18:97:54:31:1b:70:1f:7d:5c:08:23:6f:e3:c9:9f (0) b8:81:c0:36:af:60:19:7a:8b:94:15:2b:9f:82:b4:81 (0)
43:2b:b0:c5:93:08:e5:23:41:d9:c4:60:0e:9c:00:d3 (0) 23:e3:ff:70:29:cb:3a:c7:16:dc:0a:e8:a3:f8:1c:8c (0) b1:f0:0d:cb:46:4d:96:41:d7:b2:44:c3:81:be:99:b9
(1)CERTIFICATE_1 _ (1)Version 3_(0x2) (1)Serial_Number _7f:b6:a0:ea:55:e2:8c:04:4c:95:2e:95:d6:34:9f:5c_ (1)Signature_Algorithm sha256WithRSAEncryptio
(1)ISSUER_NAME _ organizationalUnitName GlobalSign_Root_CA_-_R3 _organizationName GlobalSign _commonName GlobalSign (1)SUBJECT_NAME _
countryName BE _organizationName GlobalSign_nv-sa _commonName GlobalSign_Atlas_R3_DV_TLS_CA_2024_Q1 (1)Valid_From Oct_18_04:09:32_2023_G
(1)Valid_Till Oct_18_00:00:00_2025_GMT (1)Public_Key_Algorithm rsaEncryption (1)RSA_Public_Key (2048_bit) (1) _RSA_Public-Key:_(2048_bit) (1) _Modulu
(1) _00:94:46:a2:54:17:05:2e:68:70:09:bf:bd:79:95: (1) _0d:cb:1b:a8:dd:d7:5f:d6:a0:2a:a1:2f:47:45:4a: (1) _7a:6c:7b:f9:d0:3a:cf:3c:43:68:9e:2f:48:c7:82: (1) _55:
43:94:25:1b:f4:f0:f3:94:ab:01:86:f9:42: (1) _6b:b7:45:7d:fd:43:31:6f:dd:28:d8:84:48:0c:af: (1) _d0:b8:db:ab:af:7e:86:39:b3:18:5b:e2:bc:6c:d3: (1) _06:d1:12:86:22
8a:56:a6:4c:a8:56:81:3e:38: (1) _c6:99:66:44:3e:c9:70:58:38:fc:a9:bb:72:c2:83: (1) _b6:4c:c9:cc:a6:9c:4d:3b:29:a6:b3:a3:34:96:29: (1) _50:9c:12:b5:c9:a6:22:5d
18:d0:8c:ef:04:c2:43: (1) _8c:f7:98:8a:95:7c:74:6b:12:47:51:94:b9:9c:f9: (1) _04:be:ba:a9:ca:38:22:b2:40:ca:d8:44:db:e3:1a: (1)
_66:13:64:40:41:70:17:c4:cd:c5:a6:79:fd:93:13: (1) _22:d5:ab:7c:02:1b:16:c4:23:3f:a4:db:9c:53:aa: (1) _db:e2:ea:a2:6e:9f:4a:6d:b0:1d:84:3c:9d:fa:c2: (1)
_3a:bc:f6:43:4b:e4:6d:3a:6b:fe:6d:37:5a:00:f5: (1) _03:78:37:38:01:5e:ff:37:47:4e:54:c8:20:0a:9e: (1) _20:0f (1) _Exponent:_65537_(0x10001)
(1)X509v3_EXTENSIONS _ (1)X509v3_Key_Usage critical (1) _Digital_Signature,_Certificate_Sign,_CRL_Sign (1)X509v3_Extended_Key_Usage
_TLS_Web_Server_Authentication,_TLS_Web_Client_Authentication (1)X509v3_Basic_Constraints critical (1) _CA:TRUE,_pathlen:0
(1)X509v3_Subject_Key_Identifier _66:C0:C7:A3:9A:CD:FE:F3:EA:CE:4B:53:0B:61:5E:AF:33:05:B3:E1 (1)X509v3_Authority_Key_Identifier _keyid:8F:F0:4B:
7F:A8:2E:45:24:AE:4D:50:FA:63:9A:8B:DE:E2:DD:1B:BC (1)Authority_Information_Access _OCSP_-_URI:http://ocsp2.globalsign.com/rootr3 (1) _CA_Issuers_-
_URI:http://secure.globalsign.com/cacert/root-r3.crt (1)X509v3_CRL_Distribution_Points (1) _Full_Name: (1) _URI:http://crl.globalsign.com/root-r3.crl
(1)X509v3_Certificate_Policies _Policy:_2.23.140.1.2.1 (1) _Policy:_1.3.6.1.4.1.4146.10.1.3 (1)Signature (256_octets) (1) 1d:5a:11:af:98:37:f5:8f:fd:1c:c5:7c:
07:c5:69:fe (1) 00:b8:b2:af:a3:4c:86:88:27:0a:48:3d:17:34:0e:77 (1) 2f:8f:12:70:0d:47:2b:84:a4:8c:0b:e2:f1:64:fd:07 (1) c4:27:1e:7f:ee:e2:5d:0c:
33:33:f4:56:e0:33:f4:02 (1) 8e:be:be:19:75:88:b7:c5:c5:d0:7b:6a:da:a6:de:93 (1) c0:c6:c8:8c:be:f3:e4:96:ac:e5:9b:0d:9e:9c:27:e3 (1) b5:ae:63:03:97:ea:
89:28:a2:f1:35:c9:f1:67:86:d5 (1) 0c:44:8b:3a:8d:b2:ae:c2:fb:bc:bd:39:89:72:19:77 (1) 40:60:00:38:bb:c1:db:e2:0b:b9:e7:dc:da:3b:05:fc (1) bd:94:c2:9a:31:b7:bb:
2b:a7:6f:f5:41:33:38:aa (1) bc:d6:4f:d7:24:46:da:04:07:31:88:9a:1f:aa:e4:9d (1) c2:9e:30:4f:5f:dd:2a:d9:7d:8a:a9:13:fe:c6:23:ec (1) 17:5b:42:1a:6a:dc:ec:
09:d8:a6:2f:aa:cb:ae:4f:1a (1) 15:68:20:ee:c4:bf:dc:c8:ed:47:25:eb:c2:3f:de:b9 (1) aa:05:a8:4b:47:f2:81:d6:2b:18:0a:cd:1c:e7:b5:c6 (1) fa:93:26:67:5e:0a:af:
85:82:2e:e1:1f:5c:43:3c:b1

Info List

Info #1

Certificate Fingerprint:0152F86354FCA9525B280C233F7DA6CF8B5F2373C42644723226AE67238DB190

WAS Web Application Report

Security Weaknesses (14)

150210 Information Disclosure via Response Header (1)

150210 Information Disclosure via Response Header

archibus.vodacom.co.za:443/fpr/index.as

Finding #	14173440	**Severity**	Information Gathered - Level 3
Unique #	a241a754-3c99-4dd5-aa82-a8c2aac681f5		
Group	Security Weaknesses		
CWE	CWE-16, CWE-201	**Detection Date**	11 Feb 2024 21:02 GMT+0200
OWASP	A5 Security Misconfiguration		
WASC	WASC-15 APPLICATION MISCONFIGURATION		

Details

Threat

HTTP response headers like 'Server', 'X-Powered-By', 'X-AspNetVersion', 'X-AspNetMvcVersion' could disclose information about the platform and technologies used by the website. The HTTP response include one or more such headers.

Impact

The headers can potentially be used by attackers for fingerprinting and launching attacks specific to the technologies and versions used by the web application. These response headers are not necessary for production sites and should be disabled.

Solution

Disable such response headers, remove them from the response, or make sure that the header value does not contain information which could be used to fingerprint the server-side components of the web application.

Results

One or more response headers disclosing information about the application platform were present on the following pages:
(Only first 50 such pages are reported)

GET https://archibus.vodacom.co.za/fpr/index.asp response code: 404
server: Microsoft-IIS/10.0
x-powered-by: ASP.NET

GET https://archibus.vodacom.co.za/fpr/ response code: 403
server: Microsoft-IIS/10.0
x-powered-by: ASP.NET

GET https://archibus.vodacom.co.za/FPRWin/index.aspx response code: 401
Server: Microsoft-IIS/10.0
X-Powered-By: ASP.NET

GET https://archibus.vodacom.co.za/FPRWin/ response code: 401
Server: Microsoft-IIS/10.0
X-Powered-By: ASP.NET

GET https://archibus.vodacom.co.za/fpr/null response code: 404
Server: Microsoft-IIS/10.0
X-Powered-By: ASP.NET

150261 Subresource Integrity (SRI) Not Implemented (1)

150261 Subresource Integrity (SRI) Not Implemented

archibus.vodacom.co.za:443/fpr/index.as

Finding #	10510216	**Severity**	Information Gathered - Level 3
Unique #	3ea3f43d-05b3-4e39-b969-30945c5eceec		
Group	Security Weaknesses		
CWE	CWE-693	**Detection Date**	11 Feb 2024 21:02 GMT+0200
OWASP	-		

WAS Web Application Report

WASC -

Details

Threat
The integrity attribute is missing in script and/or link elements. Subresource Integrity (SRI) is a standard browser security feature that verifies the value of the integrity attribute in

Impact
Absence of SRI checks means it is impossible to verify that the third-party resources are delivered without any unexpected manipulation.

Solution
All script and link elements that load external content should include the integrity attribute to ensure that the content is trustworthy.

More information:
Subresource Integrity article by Mozilla
OWASP Third-Party JavaScript Management Cheat Sheet

Results

Externally loaded Javascript and CSS resources without integrity checks:

Parent link : https://archibus.vodacom.co.za/_Incapsula_Resource?CWUDNSAI=23&xinfo=1-22384977-0%200NNN%20RT%281699815709016%2016037%29%20q%280%20-1%20-1%200%29%20r%280%20-1%29%20B15%284%2C200%2C0%29%20U18&incident_id=767000500460857534-122447288571202689&edet=15&cinfo=04000000&rpinfo=0&mth=GET
Found following resource links without integrity checks (only first 10 links are reported)
https://fonts.googleapis.com/css2?family=Inter:wght@300;400;500;700&display=swap

Parent link : https://archibus.vodacom.co.za/_Incapsula_Resource?CWUDNSAI=23&xinfo=1-6094665-0%200NNN%20RT%281705258965358%203%29%20q%280%20-1%20-1%200%29%20r%280%20-1%29%20B15%284%2c200%2c0%29%20U18&incident_id=1686000040225142581-36747091755008257&edet=15&cinfo=04000000&rpinfo=0&mth=GET
Found following resource links without integrity checks (only first 10 links are reported)
https://fonts.googleapis.com/css2?family=Inter:wght@300;400;500;700&display=swap

Parent link : https://archibus.vodacom.co.za/_Incapsula_Resource?CWUDNSAI=23&xinfo=10-115212261-0%200NNN%20RT%281681066894793%208%29%20q%280%20-1%20-1%20-1%29%20r%280%20-1%29%20B15%284%2C200%2C0%29%20U18&incident_id=451000960203949962-566675017241401354&edet=15&cinfo=04000000&rpinfo=0&mth=GET
Found following resource links without integrity checks (only first 10 links are reported)
https://fonts.googleapis.com/css2?family=Inter:wght@300;400;500;700&display=swap

Parent link : https://archibus.vodacom.co.za/_Incapsula_Resource?CWUDNSAI=23&xinfo=10-111982213-0%200NNN%20RT%281691953299180%205%29%20q%280%20-1%20-1%20-1%29%20r%280%20-1%29%20B15%284%2c200%2c0%29%20U18&incident_id=128000730324386403-546795125435535946&edet=15&cinfo=04000000&rpinfo=0&mth=GET
Found following resource links without integrity checks (only first 10 links are reported)
https://fonts.googleapis.com/css2?family=Inter:wght@300;400;500;700&display=swap

Parent link : https://archibus.vodacom.co.za/_Incapsula_Resource?CWUDNSAI=23&xinfo=10-115214768-0%200NNN%20RT%2816810669099963%203992%29%20q%280%20-1%20-1%200%29%20r%280%20-1%29%20B15%284%2c200%2c0%29%20U18&incident_id=451000960203949962-566690908620396554&edet=15&cinfo=04000000&rpinfo=0&mth=GET
Found following resource links without integrity checks (only first 10 links are reported)
https://fonts.googleapis.com/css2?family=Inter:wght@300;400;500;700&display=swap

Parent link : https://archibus.vodacom.co.za/_Incapsula_Resource?CWUDNSAI=23&xinfo=10-129187804-0%200NNN%20RT%2817022349388293%203%29%20q%280%20-1%20-1%200%29%20r%280%20-1%29%20B15%284%2c200%2c0%29%20U18&incident_id=281001070577460321-698535035818023626&edet=15&cinfo=04000000&rpinfo=0&mth=GET
Found following resource links without integrity checks (only first 10 links are reported)
https://fonts.googleapis.com/css2?family=Inter:wght@300;400;500;700&display=swap

Parent link : https://archibus.vodacom.co.za/_Incapsula_Resource?CWUDNSAI=23&xinfo=10-126106739-0%200NNN%20RT%2816889293652043%203%29%20q%280%20-1%20-1%20-1%29%20r%280%20-1%29%20B15%284%2c200%2c0%29%20U18&incident_id=763001020386100101-604542579974543754&edet=15&cinfo=04000000&rpinfo=0&mth=GET
Found following resource links without integrity checks (only first 10 links are reported)
https://fonts.googleapis.com/css2?family=Inter:wght@300;400;500;700&display=swap

Parent link : https://archibus.vodacom.co.za/_Incapsula_Resource?CWUDNSAI=23&xinfo=11-124742921-0%200NNN%20RT%2816919534170463%202308%29%20q%280%20-1%20-1%200%29%20r%280%20-1%29%20B15%284%2C200%2C0%29%20U18&incident_id=128000730324386403-607342817005539915&edet=15&cinfo=04000000&rpinfo=0&mth=GET
Found following resource links without integrity checks (only first 10 links are reported)
https://fonts.googleapis.com/css2?family=Inter:wght@300;400;500;700&display=swap

Parent link : https://archibus.vodacom.co.za/_Incapsula_Resource?CWUDNSAI=23&xinfo=52-10807422-0%200NNN%20RT%281705258955714%2016035%29%20q%280%20-1%20-1%201%29%20r%280%20-1%29%20B15%284%2C200%2C0%29%20U18&incident_id=1686000040225142581-61846360941789492&edet=15&cinfo=04000000&rpinfo=0&mth=GET
Found following resource links without integrity checks (only first 10 links are reported)
https://fonts.googleapis.com/css2?family=Inter:wght@300;400;500;700&display=swap

Parent link : https://archibus.vodacom.co.za/_Incapsula_Resource?CWUDNSAI=23&xinfo=11-111956721-0%200NNN%20RT%281694372520954%2015878%29%20q%280%20-1%20-1%200%29%20r%280%20-1%29%20B15%284%2C200%2C0%29%20U18&incident_id=765000070362200247-534536421231100363&edet=15&cinfo=04000000&rpinfo=0&mth=GET
Found following resource links without integrity checks (only first 10 links are reported)
https://fonts.googleapis.com/css2?family=Inter:wght@300;400;500;700&display=swap

Parent link : https://archibus.vodacom.co.za/_Incapsula_Resource?CWUDNSAI=23&xinfo=59-13731742-0%200NNN%20RT%281705258955712%202737%29%20q%280%20-1%20-1%201%29%20r%280%20-1%29%20B15%284%2C200%2C0%29%20U18&incident_id=1686000040225142581-78665255304429883&edet=15&cinfo=04000000&rpinfo=0&mth=GET
Found following resource links without integrity checks (only first 10 links are reported)
https://fonts.googleapis.com/css2?family=Inter:wght@300;400;500;700&display=swap

Parent link : https://archibus.vodacom.co.za/_Incapsula_Resource?CWUDNSAI=23&xinfo=6-50760056-0%200NNN%20RT%281691953405561%209192%29%20q%280%20-1%20-1%200%29%20r%280%20-1%29%20B15%284%2C200%2C0%29%20U18&incident_id=128000730324386403-25728565218850055 0&edet=15&cinfo=04000000&rpinfo=0&mth=GET
Found following resource links without integrity checks (only first 10 links are reported)
https://fonts.googleapis.com/css2?family=Inter:wght@300;400;500;700&display=swap

Parent link : https://archibus.vodacom.co.za/_Incapsula_Resource?CWUDNSAI=23&xinfo=6-27452916-0%200NNN%20RT%281686510573218%202872%29%20q%280%20-1%20-1%200%29%20r%280%20-1%29%20B15%284%2C200%2C0%29%20U18&incident_id=1367000740168088542-142044571547144838&edet=15&cinfo=04000000&rpinfo=0&mth=GET
Found following resource links without integrity checks (only first 10 links are reported)
https://fonts.googleapis.com/css2?family=Inter:wght@300;400;500;700&display=swap

Parent link : https://archibus.vodacom.co.za/_Incapsula_Resource?CWUDNSAI=23&xinfo=6-87530002-0%200NNN%20RT%281702234929023%2013%29%20q%280%20-1%20-1%20-1%29%20r%280%20-1%29%20B15%284%2C200%2C0%29%20U18&incident_id=281001070577460321-492085024575265478&edet=15&cinfo=04000000&rpinfo=0&mth=GET
Found following resource links without integrity checks (only first 10 links are reported)
https://fonts.googleapis.com/css2?family=Inter:wght@300;400;500;700&display=swap

Parent link : https://archibus.vodacom.co.za/_Incapsula_Resource?CWUDNSAI=23&xinfo=7-38798582-0%200NNN%20RT%281686510573218%2015874%29%20q%280%20-1%20-1%200%29%20r%280%20-1%29%20B15%284%2C200%2C0%29%20U18&incident_id=1367000740168088542-199373631805395591&edet=15&cinfo=04000000&rpinfo=0&mth=GET
Found following resource links without integrity checks (only first 10 links are reported)
https://fonts.googleapis.com/css2?family=Inter:wght@300;400;500;700&display=swap

Parent link : https://archibus.vodacom.co.za/_Incapsula_Resource?CWUDNSAI=23&xinfo=7-38318934-0%200NNN%20RT%281684090979688%2011%29%20q%280%20-1%20-1%20-1%29%20r%280%20-1%29%20B15%284%2C200%2C0%29%20U18&incident_id=765001090170903434-178457729444944711&edet=15&cinfo=04000000&rpinfo=0&mth=GET
Found following resource links without integrity checks (only first 10 links are reported)
https://fonts.googleapis.com/css2?family=Inter:wght@300;400;500;700&display=swap

Parent link : https://archibus.vodacom.co.za/_Incapsula_Resource?CWUDNSAI=23&xinfo=7-45312743-0%200NNN%20RT%281696791776989%202667%29%20q%280%20-1%20-1%200%29%20r%280%20-1%29%20B15%284%2C200%2C0%29%20U18&incident_id=7660011502803116 51-263256700448808135&edet=15&cinfo=04000000&rpinfo=0&mth=GET
Found following resource links without integrity checks (only first 10 links are reported)
https://fonts.googleapis.com/css2?family=Inter:wght@300;400;500;700&display=swap

Parent link : https://archibus.vodacom.co.za/_Incapsula_Resource?CWUDNSAI=23&xinfo=7-68982489-0%200NNN%20RT%281691953407964%203%29%20q%280%20-1%20-1%200%29%20r%280%20-1%29%20B15%284%2c200%2c0%29%20U18&incident_id=128000730324386403-342838544571568711&edet=15&cinfo=04000000&rpinfo=0&mth=GET
Found following resource links without integrity checks (only first 10 links are reported)
https://fonts.googleapis.com/css2?family=Inter:wght@300;400;500;700&display=swap

Parent link : https://archibus.vodacom.co.za/_Incapsula_Resource?CWUDNSAI=23&xinfo=7-45312741-0%200NNN%20RT%281696791776969%2011%29%20q%280%20-1%20-1%20-1%29%20r%280%20-1%29%20B15%284%2C200%2C0%29%20U18&incident_id=766001150280311651-263255351829077191&edet=15&cinfo=04000000&rpinfo=0&mth=GET
Found following resource links without integrity checks (only first 10 links are reported)
https://fonts.googleapis.com/css2?family=Inter:wght@300;400;500;700&display=swap

Parent link : https://archibus.vodacom.co.za/_Incapsula_Resource?CWUDNSAI=23&xinfo=7-77442269-0%200NNN%20RT%281694372530158%203%29%20q%280%20-1%20-1%201%29%20r%280%20-1%29%20B15%284%2c200%2c0%29%20U18&incident_id=765000070362200247-368447231281136071&edet=15&cinfo=04000000&rpinfo=0&mth=GET
Found following resource links without integrity checks (only first 10 links are reported)
https://fonts.googleapis.com/css2?family=Inter:wght@300;400;500;700&display=swap
Please check there may be more pages with subresource links without integrity checks.

150202 Missing header: X-Content-Type-Options (1)

150202 Missing header: X-Content-Type-Options *archibus.vodacom.co.za:443/fpr/index.as*

Finding #	10510218	**Severity**	Information Gathered - Level 2
Unique #	673f0dba-27d6-4e2b-8adc-fc9e3d607f2a		
Group	Security Weaknesses		
CWE	CWE-16, CWE-1032	**Detection Date**	11 Feb 2024 21:02 GMT+0200
OWASP	A5 Security Misconfiguration		
WASC	WASC-15 APPLICATION MISCONFIGURATION		

Details

Threat

The X-Content-Type-Options response header is not present. WAS reports missing X-Content-Type-Options header on each crawled link for both static and dynamic responses. The scanner performs the check not only on 200 responses but 4xx and 5xx responses as well. It's also possible the QID will be reported on directory-level links.

Impact

All web browsers employ a content-sniffing algorithm that inspects the contents of HTTP responses and also occasionally overrides the MIME type provided by the server. If X-Content-Type-Options header is not present, browsers can potentially be tricked into treating non-HTML response as HTML. An attacker can then potentially leverage the functionality to perform a cross-site scripting (XSS) attack. This specific case is known as a Content-Sniffing XSS (CS-XSS) attack.

Solution

It is recommended to disable browser content sniffing by adding the X-Content-Type-Options header to the HTTP response with a value of 'nosniff'. Also, ensure that the 'Content-Type' header is set correctly on responses.

Results

X-Content-Type-Options: Header missing
Response headers on link: GET https://archibus.vodacom.co.za/fpr/index.asp response code: 404
content-encoding: gzip
content-security-policy-report-only: default-src 'self' 'unsafe-eval' 'unsafe-hashes' 'unsafe-inline' data: blob: ; form-action 'none' data: blob: ; report-uri /csp_report
content-type: text/html
date: Sun, 11 Feb 2024 19:03:21 GMT
instance: /ITG/pool_archibus_8080 10.134.16.81 8080
server: Microsoft-IIS/10.0
x-cdn: Imperva
x-frame-options: SAMEORIGIN
x-iinfo: 62-26458618-26458857 NNYY CT(166 165 0) RT(1707678197609 3448) q(0 0 0 -1) r(2 2) U11
x-powered-by: ASP.NET
Set-Cookie: visid_incap_2776849=XzGtDabQTHuVkbHOgCNGXPUZyWUAAAAAQUIPAAAAAABzHTfqgLA/hAMNNToBRAEF; HttpOnly; expires=Sun, 09-Feb-2025 22:21:08 GMT; domain=.vodacom.co.za; path=/
Set-Cookie: nlbi_2776849=1uvTSns0kGzwA8rXZU49BAAAAABumPnVc6r7kZo+kAK6WiUr; domain=.vodacom.co.za; path=/
Set-Cookie: incap_ses_1687_2776849=ArRnARTRdWEO7PgfvG1pF/UZyWUAAAAACho9ich3SZo+8LGHMtIyTQ==; domain=.vodacom.co.za; path=/
Set-Cookie: nlbi_2776849_2147483392=bdxSNQkzDQqTStFxZU49BAAAAACIDUPtWJ8TWiQ58j4j06LA; domain=.vodacom.co.za; path=/

Header missing on the following link(s):
(Only first 50 such pages are listed)

GET https://archibus.vodacom.co.za/fpr/index.asp response code: 404
GET https://archibus.vodacom.co.za/Leasure-the-deed-will-the-clipt-Angely-ands-Banq response code: 200
GET https://archibus.vodacom.co.za/_Incapsula_Resource?SWJIYLWA=719d34d31c8e3a6e6fffd425f7e032f3&ns=12&cb=1246061612 response code: 200
GET https://archibus.vodacom.co.za/fpr/ response code: 403
GET https://archibus.vodacom.co.za/_Incapsula_Resource?SWJIYLWA=719d34d31c8e3a6e6fffd425f7e032f3%22ns=7%22cb=650421431 response code: 200
GET https://archibus.vodacom.co.za/Leasure-the-deed-will-the-clipt-Angely-ands-Banq?d=archibus.vodacom.co.za response code: 200
GET https://archibus.vodacom.co.za/_Incapsula_Resource?SWJIYLWA=719d34d31c8e3a6e6fffd425f7e032f3&ns=14&cb=1544517188 response code: 200
GET https://archibus.vodacom.co.za/_Incapsula_Resource?SWJIYLWA=719d34d31c8e3a6e6fffd425f7e032f3&ns=7&cb=650421431 response code: 200
GET https://archibus.vodacom.co.za/_Incapsula_Resource?SWKMTFSR=1&e=0.11641625286643564 response code: 200
GET https://archibus.vodacom.co.za/_Incapsula_Resource?SWKMTFSR=1&e=0.7769744014860993 response code: 200
GET https://archibus.vodacom.co.za/favicon.ico response code: 200
GET https://archibus.vodacom.co.za/tomcat.css response code: 200
GET https://archibus.vodacom.co.za/docs/ response code: 404
GET https://archibus.vodacom.co.za/docs/config/ response code: 404
GET https://archibus.vodacom.co.za/examples/ response code: 404
GET https://archibus.vodacom.co.za/docs/manager-howto.html response code: 404
GET https://archibus.vodacom.co.za/docs/security-howto.html response code: 404
GET https://archibus.vodacom.co.za/docs/cluster-howto.html response code: 404
GET https://archibus.vodacom.co.za/manager/status response code: 404
GET https://archibus.vodacom.co.za/manager/html response code: 404
GET https://archibus.vodacom.co.za/host-manager/html response code: 404
GET https://archibus.vodacom.co.za/docs/appdev/ response code: 404
GET https://archibus.vodacom.co.za/docs/setup.html response code: 404
GET https://archibus.vodacom.co.za/docs/realm-howto.html response code: 404
GET https://archibus.vodacom.co.za/docs/jndi-datasource-examples-howto.html response code: 404
GET https://archibus.vodacom.co.za/docs/RELEASE-NOTES.txt response code: 404
GET https://archibus.vodacom.co.za/docs/changelog.html response code: 404
GET https://archibus.vodacom.co.za/docs/deployer-howto.html response code: 404
GET https://archibus.vodacom.co.za/docs/api/index.html response code: 404
GET https://archibus.vodacom.co.za/_Incapsula_Resource?SWJIYLWA=719d34d31c8e3a6e6fffd425f7e032f3&ns=17&cb=316413804 response code: 200
GET https://archibus.vodacom.co.za/_Incapsula_Resource?SWKMTFSR=1&e=0.12523218982415463 response code: 200
GET https://archibus.vodacom.co.za/_Incapsula_Resource?SWJIYLWA=719d34d31c8e3a6e6fffd425f7e032f3%22ns=19%22cb=811508840 response code: 200
GET https://archibus.vodacom.co.za/_Incapsula_Resource?SWJIYLWA=719d34d31c8e3a6e6fffd425f7e032f3&ns=19&cb=811508840 response code: 200
GET https://archibus.vodacom.co.za/_Incapsula_Resource?SWJIYLWA=719d34d31c8e3a6e6fffd425f7e032f3&ns=52&cb=889049359 response code: 200
GET https://archibus.vodacom.co.za/FPRWin/index.aspx response code: 401
GET https://archibus.vodacom.co.za/_Incapsula_Resource?SWJIYLWA=719d34d31c8e3a6e6fffd425f7e032f3&ns=55&cb=1029309135 response code: 200
GET https://archibus.vodacom.co.za/_Incapsula_Resource?SWJIYLWA=719d34d31c8e3a6e6fffd425f7e032f3%22ns=36%22cb=1417430954 response code: 200
GET https://archibus.vodacom.co.za/_Incapsula_Resource?SWJIYLWA=719d34d31c8e3a6e6fffd425f7e032f3&ns=36&cb=1417430954 response code: 200
GET https://archibus.vodacom.co.za/_Incapsula_Resource?SWJIYLWA=719d34d31c8e3a6e6fffd425f7e032f3%22ns=35%22cb=1583299493 response code: 200
GET https://archibus.vodacom.co.za/_Incapsula_Resource?SWKMTFSR=1&e=0.1518548352222595 response code: 200
GET https://archibus.vodacom.co.za/_Incapsula_Resource?SWKMTFSR=1&e=0.39046879017373204 response code: 200
GET https://archibus.vodacom.co.za/_Incapsula_Resource?SWJIYLWA=719d34d31c8e3a6e6fffd425f7e032f3%22ns=46%22cb=1651641838 response code: 200

GET https://archibus.vodacom.co.za/_Incapsula_Resource?SWKMTFSR=1&e=0.7202531631723876 response code: 200
GET https://archibus.vodacom.co.za/_Incapsula_Resource?SWKMTFSR=1&e=0.951256226805095 response code: 200
GET https://archibus.vodacom.co.za/_Incapsula_Resource?SWJIYLWA=719d34d31c8e3a6e6fffd425f7e032f3%22ns=62%22cb=20911158 response code: 200
GET https://archibus.vodacom.co.za/_Incapsula_Resource?SWJIYLWA=719d34d31c8e3a6e6fffd425f7e032f3%22ns=63%22cb=915183225 response code: 200
GET https://archibus.vodacom.co.za/_Incapsula_Resource?SWKMTFSR=1&e=0.2643588357059361 response code: 200
GET https://archibus.vodacom.co.za/_Incapsula_Resource?SWJIYLWA=719d34d31c8e3a6e6fffd425f7e032f3%22ns=73%22cb=290679225 response code: 200
GET https://archibus.vodacom.co.za/manager/ response code: 404
GET https://archibus.vodacom.co.za/docs/api/ response code: 404

150206 Content-Security-Policy Not Implemented (1)

150206 Content-Security-Policy Not Implemented — *archibus.vodacom.co.za:443/fpr/index.as*

Finding #	10510221	**Severity**	Information Gathered - Level 2
Unique #	b6cc9bfe-a5e0-45d5-bda3-a36ea8abba83		
Group	Security Weaknesses		
CWE	CWE-16, CWE-1032	**Detection Date**	11 Feb 2024 21:02 GMT+0200
OWASP	A5 Security Misconfiguration		
WASC	WASC-15 APPLICATION MISCONFIGURATION		

Details

Threat

No Content-Security-Policy (CSP) is specified for the page. WAS checks for the missing CSP on all static and dynamic pages. It checks for CSP in the response headers (Content-Security-Policy, X-Content-Security-Policy or X-Webkit-CSP) and in response body (http-equiv="Content-Security-Policy" meta tag).

HTTP 4xx and 5xx responses can also be susceptible to attacks such as XSS. For better security it's important to set appropriate CSP policies on 4xx and 5xx responses as well.

Impact

Content-Security Policy is a defense mechanism that can significantly reduce the risk and impact of XSS attacks in modern browsers. The CSP specification provides a set of content restrictions for web resources and a mechanism for transmitting the policy from a server to a client where the policy is enforced. When a Content Security Policy is specified, a number of default behaviors in user agents are changed; specifically inline content and JavaScript eval constructs are not interpreted without additional directives. In short, CSP allows you to create a whitelist of sources of the trusted content. The CSP policy instructs the browser to only render resources from those whitelisted sources. Even though an attacker can find a security vulnerability in the application through which to inject script, the script won't match the whitelisted sources defined in the CSP policy, and therefore will not be executed.

The absence of Content Security Policy in the response will allow the attacker to exploit vulnerabilities as the protection provided by the browser is not at all leveraged by the Web application. If secure CSP configuration is not implemented, browsers will not be able to block content-injection attacks such as Cross-Site Scripting and Clickjacking.

Solution

Appropriate CSP policies help prevent content-injection attacks such as cross-site scripting (XSS) and clickjacking. It's recommended to add secure CSP policies as a part of a defense-in-depth approach for securing web applications.

References:
- https://cheatsheetseries.owasp.org/cheatsheets/Content_Security_Policy_Cheat_Sheet.html
- https://developers.google.com/web/fundamentals/security/csp/

Results

Content-Security-Policy: Header missing
Response headers on link: GET https://archibus.vodacom.co.za/fpr/index.asp response code: 404
content-encoding: gzip
content-security-policy-report-only: default-src 'self' 'unsafe-eval' 'unsafe-hashes' 'unsafe-inline' data: blob: ; form-action 'none' data: blob: ; report-uri /csp_report
content-type: text/html
date: Sun, 11 Feb 2024 19:03:21 GMT
instance: /ITG/pool_archibus_8080 10.134.16.81 8080
server: Microsoft-IIS/10.0
x-cdn: Imperva
x-frame-options: SAMEORIGIN

x-iinfo: 62-26458618-26458857 NNYY CT(166 165 0) RT(1707678197609 3448) q(0 0 0 -1) r(2 2) U11
x-powered-by: ASP.NET
Set-Cookie: visid_incap_2776849=XzGtDabQTHuVkbHOgCNGXPUZyWUAAAAAQUIPAAAAAABzHTfqgLA/hAMNNToBRAEF; HttpOnly; expires=Sun, 09-Feb-2025 22:21:08 GMT; domain=.vodacom.co.za; path=/
Set-Cookie: nlbi_2776849=1uvTSns0kGzwA8rXZU49BAAAAABumPnVc6r7kZo+kAK6WiUr; domain=.vodacom.co.za; path=/
Set-Cookie: incap_ses_1687_2776849=ArRnARTRdWEO7PgfvG1pF/UZyWUAAAAACho9ich3SZo+8LGHMtIyTQ==; domain=.vodacom.co.za; path=/
Set-Cookie: nlbi_2776849_2147483392=bdxSNQkzDQqTStFxZU49BAAAAACIDUPtWJ8TWiQ58j4j06LA; domain=.vodacom.co.za; path=/

Header missing, but Content-Security-Policy-Report-Only header found. It allows for testing different directives to determine how the current policy can be trimmed or modified to create the most restrictive policy possible, however still allowing all required resources. CSP header missing on the link: GET https://archibus.vodacom.co.za/fpr/index.asp response code: 404

Content-Security-Policy: Header missing, but Content-Security-Policy-Report-Only header found. It allows for testing different directives to determine how the current policy can be trimmed or modified to create the most restrictive policy possible, however still allowing all required resources. CSP header missing on the link: GET https://archibus.vodacom.co.za/Leasure-the-deed-will-the-clipt-Angely-ands-Banq response code: 200

Content-Security-Policy: Header missing, but Content-Security-Policy-Report-Only header found. It allows for testing different directives to determine how the current policy can be trimmed or modified to create the most restrictive policy possible, however still allowing all required resources. CSP header missing on the link: GET https://archibus.vodacom.co.za/_Incapsula_Resource?SWJIYLWA=719d34d31c8e3a6e6fffd425f7e032f3&ns=12&cb=1246061612 response code: 200

Content-Security-Policy: Header missing, but Content-Security-Policy-Report-Only header found. It allows for testing different directives to determine how the current policy can be trimmed or modified to create the most restrictive policy possible, however still allowing all required resources. CSP header missing on the link: GET https://archibus.vodacom.co.za/fpr/ response code: 403

Content-Security-Policy: Header missing, but Content-Security-Policy-Report-Only header found. It allows for testing different directives to determine how the current policy can be trimmed or modified to create the most restrictive policy possible, however still allowing all required resources. CSP header missing on the link: GET https://archibus.vodacom.co.za/_Incapsula_Resource?SWJIYLWA=719d34d31c8e3a6e6fffd425f7e032f3%22ns=7%22cb=650421431 response code: 200

Content-Security-Policy: Header missing, but Content-Security-Policy-Report-Only header found. It allows for testing different directives to determine how the current policy can be trimmed or modified to create the most restrictive policy possible, however still allowing all required resources. CSP header missing on the link: GET https://archibus.vodacom.co.za/Leasure-the-deed-will-the-clipt-Angely-ands-Banq?d=archibus.vodacom.co.za response code: 200

Content-Security-Policy: Header missing, but Content-Security-Policy-Report-Only header found. It allows for testing different directives to determine how the current policy can be trimmed or modified to create the most restrictive policy possible, however still allowing all required resources. CSP header missing on the link: GET https://archibus.vodacom.co.za/_Incapsula_Resource?SWJIYLWA=719d34d31c8e3a6e6fffd425f7e032f3&ns=14&cb=1544517188 response code: 200

Content-Security-Policy: Header missing, but Content-Security-Policy-Report-Only header found. It allows for testing different directives to determine how the current policy can be trimmed or modified to create the most restrictive policy possible, however still allowing all required resources. CSP header missing on the link: GET https://archibus.vodacom.co.za/_Incapsula_Resource?SWJIYLWA=719d34d31c8e3a6e6fffd425f7e032f3&ns=7&cb=650421431 response code: 200

Content-Security-Policy: Header missing, but Content-Security-Policy-Report-Only header found. It allows for testing different directives to determine how the current policy can be trimmed or modified to create the most restrictive policy possible, however still allowing all required resources. CSP header missing on the link: GET https://archibus.vodacom.co.za/_Incapsula_Resource?SWKMTFSR=1&e=0.11641625286643564 response code: 200

Content-Security-Policy: Header missing, but Content-Security-Policy-Report-Only header found. It allows for testing different directives to determine how the current policy can be trimmed or modified to create the most restrictive policy possible, however still allowing all required resources. CSP header missing on the link: GET https://archibus.vodacom.co.za/_Incapsula_Resource?SWKMTFSR=1&e=0.7769744014860993 response code: 200

Content-Security-Policy: Header missing, but Content-Security-Policy-Report-Only header found. It allows for testing different directives to determine how the current policy can be trimmed or modified to create the most restrictive policy possible, however still allowing all required resources. CSP header missing on the link: GET https://archibus.vodacom.co.za/favicon.ico response code: 200

Content-Security-Policy: Header missing, but Content-Security-Policy-Report-Only header found. It allows for testing different directives to determine how the current policy can be trimmed or modified to create the most restrictive policy possible, however still allowing all required resources. CSP header missing on the link: GET https://archibus.vodacom.co.za/tomcat.css response code: 200

Content-Security-Policy: Header missing, but Content-Security-Policy-Report-Only header found. It allows for testing different directives to determine how the current policy can be trimmed or modified to create the most restrictive policy possible, however still allowing all required resources. CSP header missing on the link: GET https://archibus.vodacom.co.za/docs/ response code: 404

Content-Security-Policy: Header missing, but Content-Security-Policy-Report-Only header found. It allows for testing different directives to determine how the current policy can be trimmed or modified to create the most restrictive policy possible, however still allowing all required resources. CSP header missing on the link: GET https://archibus.vodacom.co.za/docs/config/ response code: 404

Content-Security-Policy: Header missing, but Content-Security-Policy-Report-Only header found. It allows for testing different directives to determine how the current policy can be trimmed or modified to create the most restrictive policy possible, however still allowing all required resources. CSP header missing on the link: GET https://archibus.vodacom.co.za/examples/ response code: 404

Content-Security-Policy: Header missing, but Content-Security-Policy-Report-Only header found. It allows for testing different directives to determine how the current policy can be trimmed or modified to create the most restrictive policy possible, however still allowing all required resources. CSP header missing on the link: GET https://archibus.vodacom.co.za/docs/manager-howto.html response code: 404

Content-Security-Policy: Header missing, but Content-Security-Policy-Report-Only header found. It allows for testing different directives to determine how the current policy can be trimmed or modified to create the most restrictive policy possible, however still allowing all required resources. CSP header missing on the link: GET https://archibus.vodacom.co.za/docs/security-howto.html response code: 404

Content-Security-Policy: Header missing, but Content-Security-Policy-Report-Only header found. It allows for testing different directives to determine how the current policy can be trimmed or modified to create the most restrictive policy possible, however still allowing all required resources. CSP header missing on the link: GET https://archibus.vodacom.co.za/docs/cluster-howto.html response code: 404

Content-Security-Policy: Header missing, but Content-Security-Policy-Report-Only header found. It allows for testing different directives to determine how the current policy can be trimmed or modified to create the most restrictive policy possible, however still allowing all required resources. CSP header missing on the link: GET https://archibus.vodacom.co.za/manager/status response code: 404

Content-Security-Policy: Header missing, but Content-Security-Policy-Report-Only header found. It allows for testing different directives to determine how the current policy can be trimmed or modified to create the most restrictive policy possible, however still allowing all required resources. CSP header missing on the link: GET https://archibus.vodacom.co.za/manager/html response code: 404

Content-Security-Policy: Header missing, but Content-Security-Policy-Report-Only header found. It allows for testing different directives to determine how the current policy can be trimmed or modified to create the most restrictive policy possible, however still allowing all required resources. CSP header missing on the link: GET https://archibus.vodacom.co.za/host-manager/html response code: 404

Content-Security-Policy: Header missing, but Content-Security-Policy-Report-Only header found. It allows for testing different directives to determine how the current policy can be trimmed or modified to create the most restrictive policy possible, however still allowing all required resources. CSP header missing on the link: GET https://archibus.vodacom.co.za/docs/appdev/ response code: 404

Content-Security-Policy: Header missing, but Content-Security-Policy-Report-Only header found. It allows for testing different directives to determine how the current policy can be trimmed or modified to create the most restrictive policy possible, however still allowing all required resources. CSP header missing on the link: GET https://archibus.vodacom.co.za/docs/setup.html response code: 404

Content-Security-Policy: Header missing, but Content-Security-Policy-Report-Only header found. It allows for testing different directives to determine how the current policy can be trimmed or modified to create the most restrictive policy possible, however still allowing all required resources. CSP header missing on the link: GET https://archibus.vodacom.co.za/docs/realm-howto.html response code: 404

Content-Security-Policy: Header missing, but Content-Security-Policy-Report-Only header found. It allows for testing different directives to determine how the current policy can be trimmed or modified to create the most restrictive policy possible, however still allowing all required resources. CSP header missing on the link: GET https://archibus.vodacom.co.za/docs/jndi-datasource-examples-howto.html response code: 404

Content-Security-Policy: Header missing, but Content-Security-Policy-Report-Only header found. It allows for testing different directives to determine how the current policy can be trimmed or modified to create the most restrictive policy possible, however still allowing all required resources. CSP header missing on the link: GET https://archibus.vodacom.co.za/docs/RELEASE-NOTES.txt response code: 404

Content-Security-Policy: Header missing, but Content-Security-Policy-Report-Only header found. It allows for testing different directives to determine how the current policy can be trimmed or modified to create the most restrictive policy possible, however still allowing all required resources. CSP header missing on the link: GET https://archibus.vodacom.co.za/docs/changelog.html response code: 404

Content-Security-Policy: Header missing, but Content-Security-Policy-Report-Only header found. It allows for testing different directives to determine how the current policy can be trimmed or modified to create the most restrictive policy possible, however still allowing all required resources. CSP header missing on the link: GET https://archibus.vodacom.co.za/docs/deployer-howto.html response code: 404

Content-Security-Policy: Header missing, but Content-Security-Policy-Report-Only header found. It allows for testing different directives to determine how the current policy can be trimmed or modified to create the most restrictive policy possible, however still allowing all required resources. CSP header missing on the link: GET https://archibus.vodacom.co.za/docs/api/index.html response code: 404

Content-Security-Policy: Header missing, but Content-Security-Policy-Report-Only header found. It allows for testing different directives to determine how the current policy can be trimmed or modified to create the most restrictive policy possible, however still allowing all required resources. CSP header missing on the link: GET https://archibus.vodacom.co.za/_Incapsula_Resource?SWJIYLWA=719d34d31c8e3a6e6fffd425f7e032f3&ns=17&cb=316413804 response code: 200

Content-Security-Policy: Header missing, but Content-Security-Policy-Report-Only header found. It allows for testing different directives to determine how the current policy can be trimmed or modified to create the most restrictive policy possible, however still allowing all required resources. CSP header missing on the link: GET https://archibus.vodacom.co.za/_Incapsula_Resource?SWKMTFSR=1&e=0.12523218982415463 response code: 200

Content-Security-Policy: Header missing, but Content-Security-Policy-Report-Only header found. It allows for testing different directives to determine how the current policy can be trimmed or modified to create the most restrictive policy possible, however still allowing all required resources. CSP header missing on the link: GET https://archibus.vodacom.co.za/_Incapsula_Resource?SWJIYLWA=719d34d31c8e3a6e6fffd425f7e032f3%22ns=19%22cb=811508840 response code: 200

Content-Security-Policy: Header missing, but Content-Security-Policy-Report-Only header found. It allows for testing different directives to determine how the current policy can be trimmed or modified to create the most restrictive policy possible, however still allowing all required resources. CSP header missing on the link: GET https://archibus.vodacom.co.za/_Incapsula_Resource?SWJIYLWA=719d34d31c8e3a6e6fffd425f7e032f3&ns=19&cb=811508840 response code: 200

Content-Security-Policy: Header missing, but Content-Security-Policy-Report-Only header found. It allows for testing different directives to determine how the current policy can be trimmed or modified to create the most restrictive policy possible, however still allowing all required resources. CSP header missing on the link: GET https://archibus.vodacom.co.za/_Incapsula_Resource?SWJIYLWA=719d34d31c8e3a6e6fffd425f7e032f3&ns=52&cb=889049359 response code: 200

Content-Security-Policy: Header missing, but Content-Security-Policy-Report-Only header found. It allows for testing different directives to determine how the current policy can be trimmed or modified to create the most restrictive policy possible, however still allowing all required resources. CSP header missing on the link: GET https://archibus.vodacom.co.za/FPRWin/index.aspx response code: 401

Content-Security-Policy: Header missing, but Content-Security-Policy-Report-Only header found. It allows for testing different directives to determine how the current policy can be trimmed or modified to create the most restrictive policy possible, however still allowing all required resources. CSP header missing on the link: GET https://archibus.vodacom.co.za/_Incapsula_Resource?SWJIYLWA=719d34d31c8e3a6e6fffd425f7e032f3&ns=55&cb=1029309135 response code: 200

Content-Security-Policy: Header missing, but Content-Security-Policy-Report-Only header found. It allows for testing different directives to determine how the current policy can be trimmed or modified to create the most restrictive policy possible, however still allowing all required resources. CSP header missing on the link: GET https://archibus.vodacom.co.za/_Incapsula_Resource?SWJIYLWA=719d34d31c8e3a6e6fffd425f7e032f3%22ns=36%22cb=1417430954 response code: 200

Content-Security-Policy: Header missing, but Content-Security-Policy-Report-Only header found. It allows for testing different directives to determine how the current policy can be trimmed or modified to create the most restrictive policy possible, however still allowing all required resources. CSP header missing on the link: GET https://archibus.vodacom.co.za/_Incapsula_Resource?SWJIYLWA=719d34d31c8e3a6e6fffd425f7e032f3&ns=36&cb=1417430954 response code: 200

Content-Security-Policy: Header missing, but Content-Security-Policy-Report-Only header found. It allows for testing different directives to determine how the current policy can be trimmed or modified to create the most restrictive policy possible, however still allowing all required resources. CSP header missing on the link: GET https://archibus.vodacom.co.za/_Incapsula_Resource?SWJIYLWA=719d34d31c8e3a6e6fffd425f7e032f3%22ns=35%22cb=1583299493 response code: 200

Content-Security-Policy: Header missing, but Content-Security-Policy-Report-Only header found. It allows for testing different directives to determine how the current policy can be trimmed or modified to create the most restrictive policy possible, however still allowing all required resources. CSP header missing on the link: GET https://archibus.vodacom.co.za/_Incapsula_Resource?SWKMTFSR=1&e=0.1518548352222595 response code: 200

Content-Security-Policy: Header missing, but Content-Security-Policy-Report-Only header found. It allows for testing different directives to determine how the current policy can be trimmed or modified to create the most restrictive policy possible, however still allowing all required resources. CSP header missing on the link: GET https://archibus.vodacom.co.za/_Incapsula_Resource?SWKMTFSR=1&e=0.39046879017373204 response code: 200

Content-Security-Policy: Header missing, but Content-Security-Policy-Report-Only header found. It allows for testing different directives to determine how the current policy can be trimmed or modified to create the most restrictive policy possible, however still allowing all required resources. CSP header missing on the link: GET https://archibus.vodacom.co.za/_Incapsula_Resource?SWJIYLWA=719d34d31c8e3a6e6fffd425f7e032f3%22ns=46%22cb=1651641838 response code: 200

Content-Security-Policy: Header missing, but Content-Security-Policy-Report-Only header found. It allows for testing different directives to determine how the current policy can be trimmed or modified to create the most restrictive policy possible, however still allowing all required resources. CSP header missing on the link: GET https://archibus.vodacom.co.za/_Incapsula_Resource?SWKMTFSR=1&e=0.7202531631723876 response code: 200

Content-Security-Policy: Header missing, but Content-Security-Policy-Report-Only header found. It allows for testing different directives to determine how the current policy can be trimmed or modified to create the most restrictive policy possible, however still allowing all required resources. CSP header missing on the link: GET https://archibus.vodacom.co.za/_Incapsula_Resource?SWKMTFSR=1&e=0.951256226805095 response code: 200

Content-Security-Policy: Header missing, but Content-Security-Policy-Report-Only header found. It allows for testing different directives to determine how the current policy can be trimmed or modified to create the most restrictive policy possible, however still allowing all required resources. CSP header missing on the link: GET https://archibus.vodacom.co.za/_Incapsula_Resource?SWJIYLWA=719d34d31c8e3a6e6fffd425f7e032f3%22ns=62%22cb=20911158 response code: 200

Content-Security-Policy: Header missing, but Content-Security-Policy-Report-Only header found. It allows for testing different directives to determine how the current policy can be trimmed or modified to create the most restrictive policy possible, however still allowing all required resources. CSP header missing on the link: GET https://archibus.vodacom.co.za/_Incapsula_Resource?SWJIYLWA=719d34d31c8e3a6e6fffd425f7e032f3%22ns=63%22cb=915183225 response code: 200

Content-Security-Policy: Header missing, but Content-Security-Policy-Report-Only header found. It allows for testing different directives to determine how the current policy can be trimmed or modified to create the most restrictive policy possible, however still allowing all required resources. CSP header missing on the link: GET https://archibus.vodacom.co.za/_Incapsula_Resource?SWKMTFSR=1&e=0.2643588357059361 response code: 200

Content-Security-Policy: Header missing, but Content-Security-Policy-Report-Only header found. It allows for testing different directives to determine how the current policy can be trimmed or modified to create the most restrictive policy possible, however still allowing all required resources. CSP header missing on the link: GET https://archibus.vodacom.co.za/_Incapsula_Resource?SWJIYLWA=719d34d31c8e3a6e6fffd425f7e032f3%22ns=73%22cb=290679225 response code: 200

Content-Security-Policy: Header missing, but Content-Security-Policy-Report-Only header found. It allows for testing different directives to determine how the current policy can be trimmed or modified to create the most restrictive policy possible, however still allowing all required resources. CSP header missing on the link: GET https://archibus.vodacom.co.za/manager/ response code: 404

Content-Security-Policy: Header missing, but Content-Security-Policy-Report-Only header found. It allows for testing different directives to determine how the current policy can be trimmed or modified to create the most restrictive policy possible, however still allowing all required resources. CSP header missing on the link: GET https://archibus.vodacom.co.za/docs/api/ response code: 404

150208 Missing header: Referrer-Policy (1)

150208 Missing header: Referrer-Policy — *archibus.vodacom.co.za:443/fpr/index.as*

Finding #	10510001	**Severity**	Information Gathered - Level 2
Unique #	b51c8d4f-fd3b-4c1b-84ef-1dd7a0ec8062		
Group	Security Weaknesses		
CWE	CWE-16, CWE-1032	**Detection Date**	11 Feb 2024 21:02 GMT+0200
OWASP	A5 Security Misconfiguration		
WASC	WASC-15 APPLICATION MISCONFIGURATION		

Details

Threat

No Referrer Policy is specified for the link. WAS checks for the missing Referrer Policy on all static and dynamic pages. It checks for one of the following Referrer Policy in the response headers:

1) no-referrer
2) no-referrer-when-downgrade
3) same-origin
4) origin
5) origin-when-cross-origin
6) strict-origin
7) strict-origin-when-cross-origin

If the Referrer Policy header is not found , WAS checks in response body for meta tag containing tag name as "referrer" and one of the above Referrer Policy.

Impact

The Referrer-Policy header controls how much referrer information is sent to a site when navigating to it. Absence of Referrer-Policy header can lead to leakage of sensitive information via the referrer header.

Solution

Referrer Policy header improves security by ensuring websites don't leak sensitive information via the referrer header. It's recommended to add secure Referrer Policies as a part of a defense-in-depth approach.

References:
- https://www.w3.org/TR/referrer-policy/
- https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/Referrer-Policy

Results

Referrer-Policy: Header missing
Response headers on link: GET https://archibus.vodacom.co.za/fpr/index.asp response code: 404
content-encoding: gzip
content-security-policy-report-only: default-src 'self' 'unsafe-eval' 'unsafe-hashes' 'unsafe-inline' data: blob: ; form-action 'none' data: blob: ; report-uri /csp_report
content-type: text/html
date: Sun, 11 Feb 2024 19:03:21 GMT
instance: /ITG/pool_archibus_8080 10.134.16.81 8080
server: Microsoft-IIS/10.0
x-cdn: Imperva
x-frame-options: SAMEORIGIN
x-iinfo: 62-26458618-26458857 NNYY CT(166 165 0) RT(1707678197609 3448) q(0 0 0 -1) r(2 2) U11
x-powered-by: ASP.NET
Set-Cookie: visid_incap_2776849=XzGtDabQTHuVkbHOgCNGXPUZyWUAAAAAQUIPAAAAAABzHTfqgLA/hAMNNToBRAEF; HttpOnly; expires=Sun, 09-Feb-2025 22:21:08 GMT; domain=.vodacom.co.za; path=/
Set-Cookie: nlbi_2776849=1uvTSns0kGzwA8rXZU49BAAAAABumPnVc6r7kZo+kAK6WiUr; domain=.vodacom.co.za; path=/
Set-Cookie: incap_ses_1687_2776849=ArRnARTRdWEO7PgfvG1pF/UZyWUAAAAACho9ich3SZo+8LGHMtIyTQ==; domain=.vodacom.co.za; path=/
Set-Cookie: nlbi_2776849_2147483392=bdxSNQkzDQqTStFxZU49BAAAAACIDUPtWJ8TWiQ58j4j06LA; domain=.vodacom.co.za; path=/

Header missing on the following link(s):
(Only first 50 such pages are listed)

GET https://archibus.vodacom.co.za/fpr/index.asp response code: 404
GET https://archibus.vodacom.co.za/Leasure-the-deed-will-the-clipt-Angely-ands-Banq response code: 200
GET https://archibus.vodacom.co.za/_Incapsula_Resource?SWJIYLWA=719d34d31c8e3a6e6fffd425f7e032f3&ns=12&cb=1246061612 response code: 200
GET https://archibus.vodacom.co.za/fpr/ response code: 403
GET https://archibus.vodacom.co.za/_Incapsula_Resource?SWJIYLWA=719d34d31c8e3a6e6fffd425f7e032f3%22ns=7%22cb=650421431 response code: 200
GET https://archibus.vodacom.co.za/Leasure-the-deed-will-the-clipt-Angely-ands-Banq?d=archibus.vodacom.co.za response code: 200
GET https://archibus.vodacom.co.za/_Incapsula_Resource?SWJIYLWA=719d34d31c8e3a6e6fffd425f7e032f3&ns=14&cb=1544517188 response code: 200
GET https://archibus.vodacom.co.za/_Incapsula_Resource?SWJIYLWA=719d34d31c8e3a6e6fffd425f7e032f3&ns=7&cb=650421431 response code: 200
GET https://archibus.vodacom.co.za/_Incapsula_Resource?SWKMTFSR=1&e=0.11641625286643564 response code: 200
GET https://archibus.vodacom.co.za/_Incapsula_Resource?SWKMTFSR=1&e=0.7769744014860993 response code: 200
GET https://archibus.vodacom.co.za/favicon.ico response code: 200
GET https://archibus.vodacom.co.za/tomcat.css response code: 200
GET https://archibus.vodacom.co.za/docs/ response code: 404
GET https://archibus.vodacom.co.za/docs/config/ response code: 404
GET https://archibus.vodacom.co.za/examples/ response code: 404
GET https://archibus.vodacom.co.za/docs/manager-howto.html response code: 404
GET https://archibus.vodacom.co.za/docs/security-howto.html response code: 404
GET https://archibus.vodacom.co.za/docs/cluster-howto.html response code: 404
GET https://archibus.vodacom.co.za/manager/status response code: 404
GET https://archibus.vodacom.co.za/manager/html response code: 404
GET https://archibus.vodacom.co.za/host-manager/html response code: 404
GET https://archibus.vodacom.co.za/docs/appdev/ response code: 404
GET https://archibus.vodacom.co.za/docs/setup.html response code: 404
GET https://archibus.vodacom.co.za/docs/realm-howto.html response code: 404
GET https://archibus.vodacom.co.za/docs/jndi-datasource-examples-howto.html response code: 404
GET https://archibus.vodacom.co.za/docs/RELEASE-NOTES.txt response code: 404
GET https://archibus.vodacom.co.za/docs/changelog.html response code: 404
GET https://archibus.vodacom.co.za/docs/deployer-howto.html response code: 404
GET https://archibus.vodacom.co.za/docs/api/index.html response code: 404
GET https://archibus.vodacom.co.za/_Incapsula_Resource?SWJIYLWA=719d34d31c8e3a6e6fffd425f7e032f3&ns=17&cb=316413804 response code: 200
GET https://archibus.vodacom.co.za/_Incapsula_Resource?SWKMTFSR=1&e=0.12523218982415463 response code: 200
GET https://archibus.vodacom.co.za/_Incapsula_Resource?SWJIYLWA=719d34d31c8e3a6e6fffd425f7e032f3%22ns=19%22cb=811508840 response code: 200
GET https://archibus.vodacom.co.za/_Incapsula_Resource?SWJIYLWA=719d34d31c8e3a6e6fffd425f7e032f3&ns=19&cb=811508840 response code: 200
GET https://archibus.vodacom.co.za/_Incapsula_Resource?SWJIYLWA=719d34d31c8e3a6e6fffd425f7e032f3&ns=52&cb=889049359 response code: 200
GET https://archibus.vodacom.co.za/FPRWin/index.aspx response code: 401
GET https://archibus.vodacom.co.za/_Incapsula_Resource?SWJIYLWA=719d34d31c8e3a6e6fffd425f7e032f3&ns=55&cb=1029309135 response code: 200
GET https://archibus.vodacom.co.za/_Incapsula_Resource?SWJIYLWA=719d34d31c8e3a6e6fffd425f7e032f3%22ns=36%22cb=1417430954 response code: 200
GET https://archibus.vodacom.co.za/_Incapsula_Resource?SWJIYLWA=719d34d31c8e3a6e6fffd425f7e032f3&ns=36&cb=1417430954 response code: 200
GET https://archibus.vodacom.co.za/_Incapsula_Resource?SWJIYLWA=719d34d31c8e3a6e6fffd425f7e032f3%22ns=35%22cb=1583299493 response code: 200
GET https://archibus.vodacom.co.za/_Incapsula_Resource?SWKMTFSR=1&e=0.1518548352222595 response code: 200
GET https://archibus.vodacom.co.za/_Incapsula_Resource?SWKMTFSR=1&e=0.39046879017373204 response code: 200
GET https://archibus.vodacom.co.za/_Incapsula_Resource?SWJIYLWA=719d34d31c8e3a6e6fffd425f7e032f3%22ns=46%22cb=1651641838 response code: 200
GET https://archibus.vodacom.co.za/_Incapsula_Resource?SWKMTFSR=1&e=0.7202531631723876 response code: 200
GET https://archibus.vodacom.co.za/_Incapsula_Resource?SWKMTFSR=1&e=0.951256226805095 response code: 200
GET https://archibus.vodacom.co.za/_Incapsula_Resource?SWJIYLWA=719d34d31c8e3a6e6fffd425f7e032f3%22ns=62%22cb=20911158 response code: 200
GET https://archibus.vodacom.co.za/_Incapsula_Resource?SWJIYLWA=719d34d31c8e3a6e6fffd425f7e032f3%22ns=63%22cb=915183225 response code: 200
GET https://archibus.vodacom.co.za/_Incapsula_Resource?SWKMTFSR=1&e=0.2643588357059361 response code: 200
GET https://archibus.vodacom.co.za/_Incapsula_Resource?SWJIYLWA=719d34d31c8e3a6e6fffd425f7e032f3%22ns=73%22cb=290679225 response code: 200
GET https://archibus.vodacom.co.za/manager/ response code: 404
GET https://archibus.vodacom.co.za/docs/api/ response code: 404

WAS Web Application Report

150248 Missing header: Permissions-Policy (1)

150248 Missing header: Permissions-Policy *archibus.vodacom.co.za:443/fpr/index.as*

Finding #	10510209	**Severity**	Information Gathered - Level 2
Unique #	2cc0eea9-4091-44a9-be7a-787148af8057		
Group	Security Weaknesses		
CWE	CWE-284	**Detection Date**	11 Feb 2024 21:02 GMT+0200
OWASP	A5 Security Misconfiguration		
WASC	-		

Details

Threat

The Permissions-Policy response header is not present.

Impact

Permissions-Policy allows web developers to selectively enable, disable, or modify the behavior of some of the browser features and APIs within their application.

A user agent has a set of supported features(Policy Controlled Features), which is the set of features which it allows to be controlled through policies.

Not defining policy for unused and risky policy controlled features may leave application vulnerable.

Solution

It is recommended to define policy for policy controlled features to make application more secure.

References:
Permissions-Policy W3C Working Draft
Policy Controlled Features

Results

Permissions-Policy: Header missing
Response headers on link: GET https://archibus.vodacom.co.za/fpr/index.asp response code: 404
content-encoding: gzip
content-security-policy-report-only: default-src 'self' 'unsafe-eval' 'unsafe-hashes' 'unsafe-inline' data: blob: ; form-action 'none' data: blob: ; report-uri /csp_report
content-type: text/html
date: Sun, 11 Feb 2024 19:03:21 GMT
instance: /ITG/pool_archibus_8080 10.134.16.81 8080
server: Microsoft-IIS/10.0
x-cdn: Imperva
x-frame-options: SAMEORIGIN
x-iinfo: 62-26458618-26458857 NNYY CT(166 165 0) RT(1707678197609 3448) q(0 0 0 -1) r(2 2) U11
x-powered-by: ASP.NET
Set-Cookie: visid_incap_2776849=XzGtDabQTHuVkbHOgCNGXPUZyWUAAAAAQUIPAAAAAABzHTfqgLA/hAMNNToBRAEF; HttpOnly; expires=Sun, 09-Feb-2025 22:21:08 GMT; domain=.vodacom.co.za; path=/
Set-Cookie: nlbi_2776849=1uvTSns0kGzwA8rXZU49BAAAAABumPnVc6r7kZo+kAK6WiUr; domain=.vodacom.co.za; path=/
Set-Cookie: incap_ses_1687_2776849=ArRnARTRdWEO7PgfvG1pF/UZyWUAAAAACho9ich3SZo+8LGHMtIyTQ==; domain=.vodacom.co.za; path=/
Set-Cookie: nlbi_2776849_2147483392=bdxSNQkzDQqTStFxZU49BAAAAACIDUPtWJ8TWiQ58j4j06LA; domain=.vodacom.co.za; path=/

Header missing on the following link(s):
(Only first 50 such pages are listed)

GET https://archibus.vodacom.co.za/fpr/index.asp response code: 404
GET https://archibus.vodacom.co.za/Leasure-the-deed-will-the-clipt-Angely-ands-Banq response code: 200
GET https://archibus.vodacom.co.za/_Incapsula_Resource?SWJIYLWA=719d34d31c8e3a6e6fffd425f7e032f3&ns=12&cb=1246061612 response code: 200
GET https://archibus.vodacom.co.za/fpr/ response code: 403
GET https://archibus.vodacom.co.za/_Incapsula_Resource?SWJIYLWA=719d34d31c8e3a6e6fffd425f7e032f3%22ns=7%22cb=650421431 response code: 200
GET https://archibus.vodacom.co.za/Leasure-the-deed-will-the-clipt-Angely-ands-Banq?d=archibus.vodacom.co.za response code: 200
GET https://archibus.vodacom.co.za/_Incapsula_Resource?SWJIYLWA=719d34d31c8e3a6e6fffd425f7e032f3&ns=14&cb=1544517188 response code: 200
GET https://archibus.vodacom.co.za/_Incapsula_Resource?SWJIYLWA=719d34d31c8e3a6e6fffd425f7e032f3&ns=7&cb=650421431 response code: 200

GET https://archibus.vodacom.co.za/_Incapsula_Resource?SWKMTFSR=1&e=0.11641625286643564 response code: 200
GET https://archibus.vodacom.co.za/_Incapsula_Resource?SWKMTFSR=1&e=0.7769744014860993 response code: 200
GET https://archibus.vodacom.co.za/favicon.ico response code: 200
GET https://archibus.vodacom.co.za/tomcat.css response code: 200
GET https://archibus.vodacom.co.za/docs/ response code: 404
GET https://archibus.vodacom.co.za/docs/config/ response code: 404
GET https://archibus.vodacom.co.za/examples/ response code: 404
GET https://archibus.vodacom.co.za/docs/manager-howto.html response code: 404
GET https://archibus.vodacom.co.za/docs/security-howto.html response code: 404
GET https://archibus.vodacom.co.za/docs/cluster-howto.html response code: 404
GET https://archibus.vodacom.co.za/manager/status response code: 404
GET https://archibus.vodacom.co.za/manager/html response code: 404
GET https://archibus.vodacom.co.za/host-manager/html response code: 404
GET https://archibus.vodacom.co.za/docs/appdev/ response code: 404
GET https://archibus.vodacom.co.za/docs/setup.html response code: 404
GET https://archibus.vodacom.co.za/docs/realm-howto.html response code: 404
GET https://archibus.vodacom.co.za/docs/jndi-datasource-examples-howto.html response code: 404
GET https://archibus.vodacom.co.za/docs/RELEASE-NOTES.txt response code: 404
GET https://archibus.vodacom.co.za/docs/changelog.html response code: 404
GET https://archibus.vodacom.co.za/docs/deployer-howto.html response code: 404
GET https://archibus.vodacom.co.za/docs/api/index.html response code: 404
GET https://archibus.vodacom.co.za/_Incapsula_Resource?SWJIYLWA=719d34d31c8e3a6e6fffd425f7e032f3&ns=17&cb=316413804 response code: 200
GET https://archibus.vodacom.co.za/_Incapsula_Resource?SWKMTFSR=1&e=0.12523218982415463 response code: 200
GET https://archibus.vodacom.co.za/_Incapsula_Resource?SWJIYLWA=719d34d31c8e3a6e6fffd425f7e032f3%22ns=19%22cb=811508840 response code: 200
GET https://archibus.vodacom.co.za/_Incapsula_Resource?SWJIYLWA=719d34d31c8e3a6e6fffd425f7e032f3&ns=19&cb=811508840 response code: 200
GET https://archibus.vodacom.co.za/_Incapsula_Resource?SWJIYLWA=719d34d31c8e3a6e6fffd425f7e032f3&ns=52&cb=889049359 response code: 200
GET https://archibus.vodacom.co.za/FPRWin/index.aspx response code: 401
GET https://archibus.vodacom.co.za/_Incapsula_Resource?SWJIYLWA=719d34d31c8e3a6e6fffd425f7e032f3&ns=55&cb=1029309135 response code: 200
GET https://archibus.vodacom.co.za/_Incapsula_Resource?SWJIYLWA=719d34d31c8e3a6e6fffd425f7e032f3%22ns=36%22cb=1417430954 response code: 200
GET https://archibus.vodacom.co.za/_Incapsula_Resource?SWJIYLWA=719d34d31c8e3a6e6fffd425f7e032f3&ns=36&cb=1417430954 response code: 200
GET https://archibus.vodacom.co.za/_Incapsula_Resource?SWJIYLWA=719d34d31c8e3a6e6fffd425f7e032f3%22ns=35%22cb=1583299493 response code: 200
GET https://archibus.vodacom.co.za/_Incapsula_Resource?SWKMTFSR=1&e=0.1518548352222595 response code: 200
GET https://archibus.vodacom.co.za/_Incapsula_Resource?SWKMTFSR=1&e=0.39046879017373204 response code: 200
GET https://archibus.vodacom.co.za/_Incapsula_Resource?SWJIYLWA=719d34d31c8e3a6e6fffd425f7e032f3%22ns=46%22cb=1651641838 response code: 200
GET https://archibus.vodacom.co.za/_Incapsula_Resource?SWKMTFSR=1&e=0.7202531631723876 response code: 200
GET https://archibus.vodacom.co.za/_Incapsula_Resource?SWKMTFSR=1&e=0.951256226805095 response code: 200
GET https://archibus.vodacom.co.za/_Incapsula_Resource?SWJIYLWA=719d34d31c8e3a6e6fffd425f7e032f3%22ns=62%22cb=20911158 response code: 200
GET https://archibus.vodacom.co.za/_Incapsula_Resource?SWJIYLWA=719d34d31c8e3a6e6fffd425f7e032f3%22ns=63%22cb=915183225 response code: 200
GET https://archibus.vodacom.co.za/_Incapsula_Resource?SWKMTFSR=1&e=0.2643588357059361 response code: 200
GET https://archibus.vodacom.co.za/_Incapsula_Resource?SWJIYLWA=719d34d31c8e3a6e6fffd425f7e032f3%22ns=73%22cb=290679225 response code: 200
GET https://archibus.vodacom.co.za/manager/ response code: 404
GET https://archibus.vodacom.co.za/docs/api/ response code: 404

150249 Misconfigured Header: Cache-Control (1)

150249 Misconfigured Header: Cache-Control

archibus.vodacom.co.za:443/fpr/index.as

Finding #	10958818	**Severity**	Information Gathered - Level 2
Unique #	57f7bc26-a453-4e25-b442-59981e30226d		
Group	Security Weaknesses		
CWE	CWE-525	**Detection Date**	11 Feb 2024 21:02 GMT+0200
OWASP	A5 Security Misconfiguration		
WASC	-		

Details

Threat

Cache-Control header present but directives may not configured to adequately safeguard sensitive information.

For Example:
Cache-Control directive set to public.

max-age value is greater than 86400.

Impact

If directive is set to public, the resource can be stored by any cache.

If max-age value is greater than 86400 for sensitive information may lead to information leakage.

Solution

Please check that resources with sensitive information are not configured with Cache-Control public directive.

Also please make sure that max-age directive value set properly to not cache sensitive information for longer period than needed.

References:
Mozilla Documentation Cache-Control

Results

Cache-Control: Header misconfigured. Cache-Control public directive found.
Cache-Control:max-age=48, public on the link: GET https://archibus.vodacom.co.za/Leasure-the-deed-will-the-clipt-Angely-ands-Banq response code: 200

Cache-Control: Header misconfigured. Cache-Control public directive found.
Cache-Control:max-age=16, public on the link: GET https://archibus.vodacom.co.za/Leasure-the-deed-will-the-clipt-Angely-ands-Banq?d=archibus.vodacom.co.za response code: 200

Cache-Control: Header misconfigured. Cache-Control public directive found.
Cache-Control:max-age=86343, public on the link: GET https://archibus.vodacom.co.za/favicon.ico response code: 200

Cache-Control: Header misconfigured. Cache-Control public directive found.
Cache-Control:max-age=86360, public on the link: GET https://archibus.vodacom.co.za/tomcat.css response code: 200

150262 Missing header: Feature-Policy (1)

150262 Missing header: Feature-Policy

archibus.vodacom.co.za:443/fpr/index.as

Finding #	10510214	**Severity**	Information Gathered - Level 2
Unique #	8688feaf-485f-48f7-b103-7ca90b57b763		
Group	Security Weaknesses		
CWE	CWE-16, CWE-1032	**Detection Date**	11 Feb 2024 21:02 GMT+0200
OWASP	A5 Security Misconfiguration		
WASC	WASC-15 APPLICATION MISCONFIGURATION		

Details

Threat

The Feature-Policy response header is not present.

Impact

Feature Policy allows web developers to selectively enable, disable, and modify the behavior of certain APIs and web features such as "geolocation","camera", "usb", "fullscreen", "animations" etc in the browser.

These policies restrict what APIs the site can access or modify the browser's default behavior for certain features.

Solution

It is recommended to set the Feature-Policy header to selectively enable, disable, and modify the behavior of certain APIs and web features.

References:
- https://www.w3.org/TR/feature-policy/
- https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/Feature-Policy

Results

Feature-Policy: Header missing
Response headers on link: GET https://archibus.vodacom.co.za/fpr/index.asp response code: 404

content-encoding: gzip
content-security-policy-report-only: default-src 'self' 'unsafe-eval' 'unsafe-hashes' 'unsafe-inline' data: blob: ; form-action 'none' data: blob: ; report-uri /csp_report
content-type: text/html
date: Sun, 11 Feb 2024 19:03:21 GMT
instance: /ITG/pool_archibus_8080 10.134.16.81 8080
server: Microsoft-IIS/10.0
x-cdn: Imperva
x-frame-options: SAMEORIGIN
x-iinfo: 62-26458618-26458857 NNYY CT(166 165 0) RT(1707678197609 3448) q(0 0 0 -1) r(2 2) U11
x-powered-by: ASP.NET
Set-Cookie: visid_incap_2776849=XzGtDabQTHuVkbHOgCNGXPUZyWUAAAAAQUIPAAAAAABzHTfqgLA/hAMNNToBRAEF; HttpOnly; expires=Sun, 09-Feb-2025 22:21:08 GMT; domain=.vodacom.co.za; path=/
Set-Cookie: nlbi_2776849=1uvTSns0kGzwA8rXZU49BAAAAABumPnVc6r7kZo+kAK6WiUr; domain=.vodacom.co.za; path=/
Set-Cookie: incap_ses_1687_2776849=ArRnARTRdWEO7PgfvG1pF/UZyWUAAAAACho9ich3SZo+8LGHMtIyTQ==; domain=.vodacom.co.za; path=/
Set-Cookie: nlbi_2776849_2147483392=bdxSNQkzDQqTStFxZU49BAAAAACIDUPtWJ8TWiQ58j4j06LA; domain=.vodacom.co.za; path=/

Header missing on the following link(s):
(Only first 50 such pages are listed)

GET https://archibus.vodacom.co.za/fpr/index.asp response code: 404
GET https://archibus.vodacom.co.za/Leasure-the-deed-will-the-clipt-Angely-ands-Banq response code: 200
GET https://archibus.vodacom.co.za/_Incapsula_Resource?SWJIYLWA=719d34d31c8e3a6e6fffd425f7e032f3&ns=12&cb=1246061612 response code: 200
GET https://archibus.vodacom.co.za/fpr/ response code: 403
GET https://archibus.vodacom.co.za/_Incapsula_Resource?SWJIYLWA=719d34d31c8e3a6e6fffd425f7e032f3%22ns=7%22cb=650421431 response code: 200
GET https://archibus.vodacom.co.za/Leasure-the-deed-will-the-clipt-Angely-ands-Banq?d=archibus.vodacom.co.za response code: 200
GET https://archibus.vodacom.co.za/_Incapsula_Resource?SWJIYLWA=719d34d31c8e3a6e6fffd425f7e032f3&ns=14&cb=1544517188 response code: 200
GET https://archibus.vodacom.co.za/_Incapsula_Resource?SWJIYLWA=719d34d31c8e3a6e6fffd425f7e032f3&ns=7&cb=650421431 response code: 200
GET https://archibus.vodacom.co.za/_Incapsula_Resource?SWKMTFSR=1&e=0.11641625286643564 response code: 200
GET https://archibus.vodacom.co.za/_Incapsula_Resource?SWKMTFSR=1&e=0.7769744014860993 response code: 200
GET https://archibus.vodacom.co.za/favicon.ico response code: 200
GET https://archibus.vodacom.co.za/tomcat.css response code: 200
GET https://archibus.vodacom.co.za/docs/ response code: 404
GET https://archibus.vodacom.co.za/docs/config/ response code: 404
GET https://archibus.vodacom.co.za/examples/ response code: 404
GET https://archibus.vodacom.co.za/docs/manager-howto.html response code: 404
GET https://archibus.vodacom.co.za/docs/security-howto.html response code: 404
GET https://archibus.vodacom.co.za/docs/cluster-howto.html response code: 404
GET https://archibus.vodacom.co.za/manager/status response code: 404
GET https://archibus.vodacom.co.za/manager/html response code: 404
GET https://archibus.vodacom.co.za/host-manager/html response code: 404
GET https://archibus.vodacom.co.za/docs/appdev/ response code: 404
GET https://archibus.vodacom.co.za/docs/setup.html response code: 404
GET https://archibus.vodacom.co.za/docs/realm-howto.html response code: 404
GET https://archibus.vodacom.co.za/docs/jndi-datasource-examples-howto.html response code: 404
GET https://archibus.vodacom.co.za/docs/RELEASE-NOTES.txt response code: 404
GET https://archibus.vodacom.co.za/docs/changelog.html response code: 404
GET https://archibus.vodacom.co.za/docs/deployer-howto.html response code: 404
GET https://archibus.vodacom.co.za/docs/api/index.html response code: 404
GET https://archibus.vodacom.co.za/_Incapsula_Resource?SWJIYLWA=719d34d31c8e3a6e6fffd425f7e032f3&ns=17&cb=316413804 response code: 200
GET https://archibus.vodacom.co.za/_Incapsula_Resource?SWKMTFSR=1&e=0.12523218982415463 response code: 200
GET https://archibus.vodacom.co.za/_Incapsula_Resource?SWJIYLWA=719d34d31c8e3a6e6fffd425f7e032f3%22ns=19%22cb=811508840 response code: 200
GET https://archibus.vodacom.co.za/_Incapsula_Resource?SWJIYLWA=719d34d31c8e3a6e6fffd425f7e032f3&ns=19&cb=811508840 response code: 200
GET https://archibus.vodacom.co.za/_Incapsula_Resource?SWJIYLWA=719d34d31c8e3a6e6fffd425f7e032f3&ns=52&cb=889049359 response code: 200
GET https://archibus.vodacom.co.za/FPRWin/index.aspx response code: 401
GET https://archibus.vodacom.co.za/_Incapsula_Resource?SWJIYLWA=719d34d31c8e3a6e6fffd425f7e032f3&ns=55&cb=1029309135 response code: 200
GET https://archibus.vodacom.co.za/_Incapsula_Resource?SWJIYLWA=719d34d31c8e3a6e6fffd425f7e032f3%22ns=36%22cb=1417430954 response code: 200
GET https://archibus.vodacom.co.za/_Incapsula_Resource?SWJIYLWA=719d34d31c8e3a6e6fffd425f7e032f3&ns=36&cb=1417430954 response code: 200
GET https://archibus.vodacom.co.za/_Incapsula_Resource?SWJIYLWA=719d34d31c8e3a6e6fffd425f7e032f3%22ns=35%22cb=1583299493 response code: 200
GET https://archibus.vodacom.co.za/_Incapsula_Resource?SWKMTFSR=1&e=0.1518548352222595 response code: 200
GET https://archibus.vodacom.co.za/_Incapsula_Resource?SWKMTFSR=1&e=0.39046879017373204 response code: 200
GET https://archibus.vodacom.co.za/_Incapsula_Resource?SWJIYLWA=719d34d31c8e3a6e6fffd425f7e032f3%22ns=46%22cb=1651641838 response code: 200
GET https://archibus.vodacom.co.za/_Incapsula_Resource?SWKMTFSR=1&e=0.7202531631723876 response code: 200
GET https://archibus.vodacom.co.za/_Incapsula_Resource?SWKMTFSR=1&e=0.951256226805095 response code: 200
GET https://archibus.vodacom.co.za/_Incapsula_Resource?SWJIYLWA=719d34d31c8e3a6e6fffd425f7e032f3%22ns=62%22cb=20911158 response code: 200
GET https://archibus.vodacom.co.za/_Incapsula_Resource?SWJIYLWA=719d34d31c8e3a6e6fffd425f7e032f3%22ns=63%22cb=915183225 response code: 200
GET https://archibus.vodacom.co.za/_Incapsula_Resource?SWKMTFSR=1&e=0.2643588357059361 response code: 200
GET https://archibus.vodacom.co.za/_Incapsula_Resource?SWJIYLWA=719d34d31c8e3a6e6fffd425f7e032f3%22ns=73%22cb=290679225 response code: 200
GET https://archibus.vodacom.co.za/manager/ response code: 404
GET https://archibus.vodacom.co.za/docs/api/ response code: 404

150126 Links With High Resource Consumption (1)

150126 Links With High Resource Consumption

archibus.vodacom.co.za:443/fpr/index.as

Finding #	10541620	**Severity**	Information Gathered - Level 1
Unique #	1ddc2374-34d7-4c18-94dc-7d1d284ff788		
Group	Security Weaknesses		
CWE	-	**Detection Date**	11 Feb 2024 21:02 GMT+0200
OWASP	-		

WASC	-

Details

Threat
The list of links with lowest bytes/sec which are assumed to be resources with highest resource consumption. The links in the list have slower transfer times speeds to an average resource on the server. This may indicate that the links are more CPU or DB intensive than majority of links.

The latency of the network and file size have no effect on calculations.

Impact
The links with high resource consumption could be used to perform DOS on the server by just performing GET Flooding. Attackers could more easily take the server down if there are huge resource hogs on it, performing less request.

Solution
Find the root cause of resources slow download speed.

If the cause is a real CPU strain or complex DB queries performed, there may be a need for re-engineering of the web application or defense measures should be in place. Examples of defense against DOS that is targeted towards high resource consumption links are Load Balancers and Rate Limiters.

Results

0.000000 bytes/sec https://archibus.vodacom.co.za/_Incapsula_Resource?SWJIYLWA=719d34d31c8e3a6e6fffd425f7e032f3%22ns=35%22cb=1583299493
0.000000 bytes/sec https://archibus.vodacom.co.za/_Incapsula_Resource?SWJIYLWA=719d34d31c8e3a6e6fffd425f7e032f3%22ns=36%22cb=1417430954
0.000000 bytes/sec https://archibus.vodacom.co.za/_Incapsula_Resource?SWJIYLWA=719d34d31c8e3a6e6fffd425f7e032f3%22ns=46%22cb=1651641838
0.000000 bytes/sec https://archibus.vodacom.co.za/_Incapsula_Resource?SWJIYLWA=719d34d31c8e3a6e6fffd425f7e032f3%22ns=62%22cb=20911158
0.000000 bytes/sec https://archibus.vodacom.co.za/_Incapsula_Resource?SWJIYLWA=719d34d31c8e3a6e6fffd425f7e032f3%22ns=63%22cb=915183225
0.000000 bytes/sec https://archibus.vodacom.co.za/_Incapsula_Resource?SWJIYLWA=719d34d31c8e3a6e6fffd425f7e032f3%22ns=7%22cb=650421431
0.000000 bytes/sec https://archibus.vodacom.co.za/_Incapsula_Resource?SWJIYLWA=719d34d31c8e3a6e6fffd425f7e032f3%22ns=83%22cb=723631670
0.000000 bytes/sec https://archibus.vodacom.co.za/_Incapsula_Resource?SWJIYLWA=719d34d31c8e3a6e6fffd425f7e032f3%22ns=84%22cb=1882006911
0.000000 bytes/sec https://archibus.vodacom.co.za/_Incapsula_Resource?SWJIYLWA=719d34d31c8e3a6e6fffd425f7e032f3%22ns=94%22cb=2073905376
0.000000 bytes/sec https://archibus.vodacom.co.za/csp_report

150135 HTTP Strict Transport Security (HSTS) header missing or misconfigured (1)

150135 HTTP Strict Transport Security (HSTS) header missing or misconfigured — *archibus.vodacom.co.za:443/fpr/index.as*

Finding #	10510215	Severity	Information Gathered - Level 1
Unique #	c0803a63-e52a-4adf-8864-8a862907ebf2		
Group	Security Weaknesses		
CWE	CWE-523	Detection Date	11 Feb 2024 21:02 GMT+0200
OWASP	A5 Security Misconfiguration		
WASC	-		

Details

Threat
HTTP Strict Transport Security (HSTS) header was found to be missing or misconfigured. The HSTS header instructs browsers that all subsequent connections to the website, for a configurable amount of time, should be performed over a secure (HTTPS) connection only. Additionally, it instructs browsers that users should not be permitted to bypass SSL/TLS certificate errors, in the event of an expired or otherwise untrusted certificate for example.

Impact
If HSTS header is not set, users are potentially vulnerable to man-in-the-middle (MITM) attacks, SSL stripping, and passive eavesdropper attacks.

Solution
For information about how to implement the HSTS header properly, refer to the OWASP HTTP Strict Transport Security Cheat Sheet.

WAS Web Application Report

Results

Strict Transport Security header missing for
https://archibus.vodacom.co.za/_Incapsula_Resource?SWKMTFSR=1&e=0.11641625286643564

150142 Virtual Host Discovered (1)

150142 Virtual Host Discovered

archibus.vodacom.co.za:443/fpr/index.as

Finding #	14173443	**Severity**	Information Gathered - Level 1
Unique #	802812ff-75e9-460a-af1c-674bd8499103		
Group	Security Weaknesses		
CWE	CWE-200	**Detection Date**	11 Feb 2024 21:02 GMT+0200
OWASP	A5 Security Misconfiguration		
WASC	-		

Details

Threat

Web server is responding differently when the HOST header is manipulated and various common virtual hosts are tested. This could indicate the presence of Virtual Host. Virtual hosting is a method for hosting multiple domain names (with separate handling of each name) on a single server (or pool of servers). This allows one server to share its resources, such as memory and processor cycles, without requiring all services provided to use the same host name. The extra virtual hosts discovered by the Web application scanner during HOST header manipulation are provided in the Results section.

Impact

The Web application should apply consistent security measures. If the Web application fails to apply security controls to other domains hosted on the same server, then it may be exposed to vulnerabilities like cross-site scripting, SQL injection, or authorization-based attacks.

Solution

Consult the virtual host configuration and check if this virtual host should be publicly accessible.

Results

Virtual host discovered:

Detected based on: HTTP Response code
Virtual Host: web.vodacom.co.za
URI: https://archibus.vodacom.co.za/

150204 Missing header: X-XSS-Protection (1)

150204 Missing header: X-XSS-Protection

archibus.vodacom.co.za:443/fpr/index.as

Finding #	10510223	**Severity**	Information Gathered - Level 1
Unique #	a17fde6d-940d-4e11-a6fb-7906e45d4434		
Group	Security Weaknesses		
CWE	CWE-16, CWE-1032	**Detection Date**	11 Feb 2024 21:02 GMT+0200
OWASP	A5 Security Misconfiguration		
WASC	WASC-15 APPLICATION MISCONFIGURATION		

Details

Threat

The X-XSS-Protection response header is not present.

Impact

The X-XSS-Protection response header provides a layer of protection against reflected cross-site scripting (XSS) attacks by instructing browsers to abort rendering a page in which a reflected XSS attack has been detected. This is a best-effort second line of defense measure which helps prevent an attacker from using evasion techniques to avoid the neutralization mechanisms that the filters use by default. When configured appropriately, browser-level XSS filters can provide additional layers of defense against web application attacks.

Note that HTTP 4xx and 5xx responses can also be susceptible to attacks such as XSS. For better security the X-XSS-Protection header should be set on 4xx and 5xx responses as well.

Solution

It is recommend to set X-XSS-Protection header with value set to '1; mode=block' on all the relevant responses to activate browser's XSS filter.

NOTE: The X-XSS-Protection header is not supported by all browsers. Google Chrome and Safari are some of the browsers which support it, Firefox on the other hand does not support the header. X-XSS-Protection header does not guarantee a complete protection against XSS. For better protection against XSS attacks, the web application should use secure coding principles. Also, consider leveraging the Content-Security-Policy (CSP) header, which is supported by all browsers.

Using X-XSS-Protection could have unintended side effects, please understand the implications carefully before using it.

References:
- https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/X-XSS-Protection
- https://blog.innerht.ml/the-misunderstood-x-xss-protection/
- https://www.mbsd.jp/blog/20160407.html
- https://www.chromium.org/developers/design-documents/xss-auditor

Results

X-Xss-Protection: Header missing
Response headers on link: GET https://archibus.vodacom.co.za/fpr/index.asp response code: 404
content-encoding: gzip
content-security-policy-report-only: default-src 'self' 'unsafe-eval' 'unsafe-hashes' 'unsafe-inline' data: blob: ; form-action 'none' data: blob: ; report-uri /csp_report
content-type: text/html
date: Sun, 11 Feb 2024 19:03:21 GMT
instance: /ITG/pool_archibus_8080 10.134.16.81 8080
server: Microsoft-IIS/10.0
x-cdn: Imperva
x-frame-options: SAMEORIGIN
x-iinfo: 62-26458618-26458857 NNYY CT(166 165 0) RT(1707678197609 3448) q(0 0 0 -1) r(2 2) U11
x-powered-by: ASP.NET
Set-Cookie: visid_incap_2776849=XzGtDabQTHuVkbHOgCNGXPUZyWUAAAAAQUIPAAAAAABzHTfqgLA/hAMNNToBRAEF; HttpOnly; expires=Sun, 09-Feb-2025 22:21:08 GMT; domain=.vodacom.co.za; path=/
Set-Cookie: nlbi_2776849=1uvTSns0kGzwA8rXZU49BAAAAABumPnVc6r7kZo+kAK6WiUr; domain=.vodacom.co.za; path=/
Set-Cookie: incap_ses_1687_2776849=ArRnARTRdWEO7PgfvG1pF/UZyWUAAAAACho9ich3SZo+8LGHMtIyTQ==; domain=.vodacom.co.za; path=/
Set-Cookie: nlbi_2776849_2147483392=bdxSNQkzDQqTStFxZU49BAAAAACIDUPtWJ8TWiQ58j4j06LA; domain=.vodacom.co.za; path=/

Header missing on the following link(s):
(Only first 50 such pages are listed)

GET https://archibus.vodacom.co.za/fpr/index.asp response code: 404
GET https://archibus.vodacom.co.za/fpr/ response code: 403
GET https://archibus.vodacom.co.za/_Incapsula_Resource?SWKMTFSR=1&e=0.11641625286643564 response code: 200
GET https://archibus.vodacom.co.za/_Incapsula_Resource?SWKMTFSR=1&e=0.7769744014860993 response code: 200
GET https://archibus.vodacom.co.za/docs/ response code: 404
GET https://archibus.vodacom.co.za/docs/config/ response code: 404
GET https://archibus.vodacom.co.za/examples/ response code: 404
GET https://archibus.vodacom.co.za/docs/manager-howto.html response code: 404
GET https://archibus.vodacom.co.za/docs/security-howto.html response code: 404
GET https://archibus.vodacom.co.za/docs/cluster-howto.html response code: 404
GET https://archibus.vodacom.co.za/manager/status response code: 404
GET https://archibus.vodacom.co.za/manager/html response code: 404
GET https://archibus.vodacom.co.za/host-manager/html response code: 404
GET https://archibus.vodacom.co.za/docs/appdev/ response code: 404
GET https://archibus.vodacom.co.za/docs/setup.html response code: 404
GET https://archibus.vodacom.co.za/docs/realm-howto.html response code: 404
GET https://archibus.vodacom.co.za/docs/jndi-datasource-examples-howto.html response code: 404
GET https://archibus.vodacom.co.za/docs/RELEASE-NOTES.txt response code: 404
GET https://archibus.vodacom.co.za/docs/changelog.html response code: 404
GET https://archibus.vodacom.co.za/docs/deployer-howto.html response code: 404
GET https://archibus.vodacom.co.za/docs/api/index.html response code: 404

GET https://archibus.vodacom.co.za/_Incapsula_Resource?SWKMTFSR=1&e=0.12523218982415463 response code: 200
GET https://archibus.vodacom.co.za/FPRWin/index.aspx response code: 401
GET https://archibus.vodacom.co.za/_Incapsula_Resource?SWKMTFSR=1&e=0.1518548352222595 response code: 200
GET https://archibus.vodacom.co.za/_Incapsula_Resource?SWKMTFSR=1&e=0.39046879017373204 response code: 200
GET https://archibus.vodacom.co.za/_Incapsula_Resource?SWKMTFSR=1&e=0.7202531631723876 response code: 200
GET https://archibus.vodacom.co.za/_Incapsula_Resource?SWKMTFSR=1&e=0.951256226805095 response code: 200
GET https://archibus.vodacom.co.za/_Incapsula_Resource?SWKMTFSR=1&e=0.2643588357059361 response code: 200
GET https://archibus.vodacom.co.za/manager/ response code: 404
GET https://archibus.vodacom.co.za/docs/api/ response code: 404
GET https://archibus.vodacom.co.za/host-manager/ response code: 404
GET https://archibus.vodacom.co.za/FPRWin/ response code: 401
GET https://archibus.vodacom.co.za/_Incapsula_Resource?CWUDNSAI=23%22xinfo=11-140064347-0%200NNN%20RT%281702234929044%203123%29%20q%280%20-1%20-1%201%29%20r%280%20-1%29%20B15%284%2c200%2c0%29%20U18%22incident_id=281001070577460321-753234837356747467%22edet=15%22cinfo=04000000%22rpinfo=0%22mth=GET response code: 404
GET https://archibus.vodacom.co.za/_Incapsula_Resource?CWUDNSAI=23%22xinfo=11-140064348-0%200NNN%20RT%281702234929044%2016190%29%20q%280%20-1%20-1%202%29%20r%280%20-1%29%20B15%284%2c200%2c0%29%20U18%22incident_id=281001070577460321-753246536847661771%22edet=15%22cinfo=04000000%22rpinfo=0%22mth=GET response code: 404
GET https://archibus.vodacom.co.za/_Incapsula_Resource?CWUDNSAI=23%22xinfo=11-124742921-0%200NNN%20RT%281691953417046%202308%29%20q%280%20-1%20-1%200%29%20r%280%20-1%29%20B15%284%2c200%2c0%29%20U18%22incident_id=128000730324386403-607342817005539915%22edet=15%22cinfo=04000000%22rpinfo=0%22mth=GET response code: 404
GET https://archibus.vodacom.co.za/_Incapsula_Resource?CWUDNSAI=23%22xinfo=14-114596260-0%200NNN%20RT%281686510589098%204193%29%20q%280%20-1%20-1%203%29%20r%280%20-1%29%20B15%284%2c200%2c0%29%20U18%22incident_id=136700074016808854-5478685280383187 34%22edet=15%22cinfo=04000000%22rpinfo=0%22mth=GET response code: 404
GET https://archibus.vodacom.co.za/_Incapsula_Resource?CWUDNSAI=23%22xinfo=14-163459825-0%200NNN%20RT%281694372520953%202886%29%20q%280%20-1%20-1%200%29%20r%280%20-1%29%20B15%284%2c200%2c0%29%20U18%22incident_id=765000070362200247-772776844095979982%22edet=15%22cinfo=04000000%22rpinfo=0%22mth=GET response code: 404
GET https://archibus.vodacom.co.za/_Incapsula_Resource?CWUDNSAI=23%22xinfo=13-70594367-0%200NNN%20RT%281696791792934%204590%29%20q%280%20-1%20-1%200%29%20r%280%20-1%29%20B15%284%2c200%2c0%29%20U18%22incident_id=766001150280311651-392210022609591501%22edet=15%22cinfo=04000000%22rpinfo=0%22mth=GET response code: 404
GET https://archibus.vodacom.co.za/_Incapsula_Resource?CWUDNSAI=23%22xinfo=13-157825945-0%200NNN%20RT%281691953421567%2015799%29%20q%280%20-1%20-1%201%29%20r%280%20-1%29%20B15%284%2c200%2c0%29%20U18%22incident_id=128000730324386403-757535280726020685%22edet=15%22cinfo=04000000%22rpinfo=0%22mth=GET response code: 404
GET https://archibus.vodacom.co.za/_Incapsula_Resource?CWUDNSAI=23%22xinfo=12-77127187-0%200NNN%20RT%281684090995888%204094%29%20q%280%20-1%20-1%200%29%20r%280%20-1%29%20B15%284%2c200%2c0%29%20U18%22incident_id=765001090170903434-359203417983097676%22edet=15%22cinfo=04000000%22rpinfo=0%22mth=GET response code: 404
GET https://archibus.vodacom.co.za/_Incapsula_Resource?CWUDNSAI=23%22xinfo=13-146013152-0%200NNN%20RT%281699815709015%202793%29%20q%280%20-1%20-1%204%29%20r%280%20-1%29%20B15%284%2c200%2c0%29%20U18%22incident_id=767000500460857534-774752327188810893%22edet=15%22cinfo=04000000%22rpinfo=0%22mth=GET response code: 404
GET https://archibus.vodacom.co.za/_Incapsula_Resource?CWUDNSAI=23%22xinfo=32-11389906-0%200NNN%20RT%281705258971756%204195%29%20q%280%20-1%20-1%201%29%20r%280%20-1%29%20B15%284%2c200%2c0%29%20U18%22incident_id=168600004022514 2581-65795549010723104%22edet=15%22cinfo=04000000%22rpinfo=0%22mth=GET response code: 404
GET https://archibus.vodacom.co.za/_Incapsula_Resource?CWUDNSAI=23%22xinfo=3-53041329-0%200NNN%20RT%281702234945242%204178%29%20q%280%20-1%20-1%200%29%20r%280%20-1%29%20B15%284%2c200%2c0%29%20U18%22incident_id=281001070577460321-313704059130944195%22edet=15%22cinfo=04000000%22rpinfo=0%22mth=GET response code: 404
GET https://archibus.vodacom.co.za/_Incapsula_Resource?CWUDNSAI=23%22xinfo=5-116739429-0%200NNN%20RT%281688929427752%202697%29%20q%280%20-1%20-1%200%29%20r%280%20-1%29%20B15%284%2c200%2c0%29%20U18%22incident_id=763001020386100101-555576851833756037%22edet=15%22cinfo=04000000%22rpinfo=0%22mth=GET response code: 404
GET https://archibus.vodacom.co.za/_Incapsula_Resource?CWUDNSAI=23%22xinfo=12-77124096-0%200NNN%20RT%281684090979706%202875%29%20q%280%20-1%20-1%200%29%20r%280%20-1%29%20B15%284%2c200%2c0%29%20U18%22incident_id=765001090170903434-35918781007194 4012%22edet=15%22cinfo=04000000%22rpinfo=0%22mth=GET response code: 404
GET https://archibus.vodacom.co.za/_Incapsula_Resource?CWUDNSAI=23%22xinfo=12-143392341-0%200NNN%20RT%281691953401023%20467%29%20q%280%20-1%20-1%201%29%20r%280%20-1%29%20B15%284%2c200%2c0%29%20U18%22incident_id=128000730324386403-688681977104044620%22edet=15%22cinfo=04000000%22rpinfo=0%22mth=GET response code: 404
GET https://archibus.vodacom.co.za/_Incapsula_Resource?CWUDNSAI=23%22xinfo=12-182571436-0%200NNN%20RT%281688929427753%2015665%29%20q%280%20-1%20-1%202%29%20r%280%20-1%29%20B15%284%2c200%2c0%29%20U18%22incident_id=763001020386100101-868537211589171596%22edet=15%22cinfo=04000000%22rpinfo=0%22mth=GET response code: 404
GET https://archibus.vodacom.co.za/_Incapsula_Resource?CWUDNSAI=23%22xinfo=2-26051945-0%200NNN%20RT%281694372536840%204197%29%20q%280%20-1%20-1%200%29%20r%280%20-1%29%20B15%284%2c200%2c0%29%20U18%22incident_id=765000070362200247-129321293534003650%22edet=15%22cinfo=04000000%22rpinfo=0%22mth=GET response code: 404
GET https://archibus.vodacom.co.za/_Incapsula_Resource?CWUDNSAI=23%22xinfo=2-16530192-0%200NNN%20RT%2816967917769 89%2015936%29%20q%280%20-1%20-1%200%29%20r%280%20-1%29%20B15%284%2c200%2c0%29%20U18%22incident_id=766001150280311651-85428939677113538%22edet=15%22cinfo=04000000%22rpinfo=0%22mth=GET response code: 404
GET https://archibus.vodacom.co.za/_Incapsula_Resource?CWUDNSAI=23%22xinfo=14-98161412-0%200NNN%20RT%281684090979710%2016171%29%20q%280%20-1%20-1%200%29%20r%280%20-1%29%20B15%284%2c200%2c0%29%20U18%22incident_id=765001090170903434-451351309958585166%22edet=15%22cinfo=04000000%22rpinfo=0%22mth=GET response code: 404

150245 Missing header: X-Frame-Options (1)

150245 Missing header: X-Frame-Options

archibus.vodacom.co.za:443/fpr/index.as

Finding #	10510206	**Severity**	Information Gathered - Level 1
Unique #	1657eb47-e47f-4954-8ad1-a77aeb7331a9		
Group	Security Weaknesses		
CWE	CWE-693	**Detection Date**	11 Feb 2024 21:02 GMT+0200
OWASP	A5 Security Misconfiguration		
WASC	WASC-15 APPLICATION MISCONFIGURATION		

WAS Web Application Report

Details

Threat

The X-Frame-Options header is not set in the HTTP response, meaning the page can potentially be loaded into an attacker-controlled frame. This could lead to clickjacking, where an attacker adds an invisible layer on top of the legitimate page to trick users into clicking on a malicious link or taking a harmful action.

Impact

Without an X-Frame-Options response header, clickjacking may be possible. However, if the application properly uses the Content-Security-Policy "frame-ancestors" directive, then modern web browsers would stop the page from being framed and prevent clickjacking.

Solution

The X-Frame-Options allows three values: DENY, SAMEORIGIN and ALLOW-FROM. It is recommended to use DENY, which prevents all domains from framing the page or SAMEORIGIN, which allows framing only by the same site. DENY and SAMEORGIN are supported by all browsers. Using ALLOW-FROM is not recommended because not all browsers support it.

Note: To avoid a common X-Frame-Options implementation mistake, see https://blog.qualys.com/securitylabs/2015/10/20/clickjacking-a-common-implementation-mistake-that-can-put-your-websites-in-danger.

Results

X-Frame-Options header is missing or not set to DENY or SAMEORIGIN for the following pages:
(Only first 10 such pages are reported)

GET https://archibus.vodacom.co.za/_Incapsula_Resource?CWUDNSAI=23&xinfo=1-22384977-0%200NNN%20RT%281699815709016%2016037%29%20q%280%20-1%20-1%200%29%20r%280%20-1%29%20B15%284%2C200%2C0%29%20U18&incident_id=767000500460857534-122447288571202689&edet=15&cinfo=04000000&rpinfo=0&mth=GET
Response code: 200
Response headers:
Cache-Control: no-cache, no-store
Content-Encoding: gzip
Content-Length: 3756
Content-Security-Policy-Report-Only: default-src 'self' 'unsafe-eval' 'unsafe-hashes' 'unsafe-inline' data: blob: ; form-action 'none' data: blob: ; report-uri /csp_report
Content-Type: text/html
X-Robots-Tag: noindex
Set-Cookie: visid_incap_2776849=XzGtDabQTHuVkbHOgCNGXPUZyWUAAAAAQUIPAAAAAABzHTfqgLA/hAMNNToBRAEF; HttpOnly; expires=Sun, 09-Feb-2025 22:21:08 GMT; domain=.vodacom.co.za; path=/
Set-Cookie: nlbi_2776849=1uvTSns0kGzwA8rXZU49BAAAAABumPnVc6r7kZo+kAK6WiUr; domain=.vodacom.co.za; path=/
Set-Cookie: incap_ses_1687_2776849=ArRnARTRdWEO7PgfvG1pF/UZyWUAAAAACho9ich3SZo+8LGHMtIyTQ==; domain=.vodacom.co.za; path=/
Set-Cookie: nlbi_2776849_2147483392=5mZ7ez+BRjupvk6+ZU49BAAAAACxj6KLVqu1zBAwGDwzNMPg; domain=.vodacom.co.za; path=/

GET https://archibus.vodacom.co.za/_Incapsula_Resource?CWUDNSAI=23&xinfo=1-6094665-0%200NNN%20RT%281705258965358%203%29%20q%280%20-1%20-1%200%29%20r%280%20-1%29%20B15%284%2c200%2c0%29%20U18&incident_id=1686000040225142581-36747091755008257&edet=15&cinfo=04000000&rpinfo=0&mth=GET
Response code: 200
Response headers:
Cache-Control: no-cache, no-store
Content-Encoding: gzip
Content-Length: 3756
Content-Security-Policy-Report-Only: default-src 'self' 'unsafe-eval' 'unsafe-hashes' 'unsafe-inline' data: blob: ; form-action 'none' data: blob: ; report-uri /csp_report
Content-Type: text/html
X-Robots-Tag: noindex
Set-Cookie: visid_incap_2776849=XzGtDabQTHuVkbHOgCNGXPUZyWUAAAAAQUIPAAAAAABzHTfqgLA/hAMNNToBRAEF; HttpOnly; expires=Sun, 09-Feb-2025 22:21:08 GMT; domain=.vodacom.co.za; path=/
Set-Cookie: nlbi_2776849=1uvTSns0kGzwA8rXZU49BAAAAABumPnVc6r7kZo+kAK6WiUr; domain=.vodacom.co.za; path=/
Set-Cookie: incap_ses_1687_2776849=ArRnARTRdWEO7PgfvG1pF/UZyWUAAAAACho9ich3SZo+8LGHMtIyTQ==; domain=.vodacom.co.za; path=/
Set-Cookie: nlbi_2776849_2147483392=5mZ7ez+BRjupvk6+ZU49BAAAAACxj6KLVqu1zBAwGDwzNMPg; domain=.vodacom.co.za; path=/

GET https://archibus.vodacom.co.za/_Incapsula_Resource?CWUDNSAI=23&xinfo=10-111982213-0%200NNN%20RT%281691953299180%205%29%20q%280%20-1%20-1%20-1%29%20r%280%20-1%29%20B15%284%2c200%2c0%29%20U18&incident_id=128000730324386403-546795125435535946&edet=15&cinfo=04000000&rpinfo=0&mth=GET
Response code: 200
Response headers:
Cache-Control: no-cache, no-store
Content-Encoding: gzip
Content-Length: 3755
Content-Security-Policy-Report-Only: default-src 'self' 'unsafe-eval' 'unsafe-hashes' 'unsafe-inline' data: blob: ; form-action 'none' data: blob: ; report-uri /csp_report
Content-Type: text/html
X-Robots-Tag: noindex
Set-Cookie: visid_incap_2776849=XzGtDabQTHuVkbHOgCNGXPUZyWUAAAAAQUIPAAAAAABzHTfqgLA/hAMNNToBRAEF; HttpOnly; expires=Sun, 09-Feb-2025 22:21:08 GMT; domain=.vodacom.co.za; path=/
Set-Cookie: nlbi_2776849=1uvTSns0kGzwA8rXZU49BAAAAABumPnVc6r7kZo+kAK6WiUr; domain=.vodacom.co.za; path=/
Set-Cookie: incap_ses_1687_2776849=ArRnARTRdWEO7PgfvG1pF/UZyWUAAAAACho9ich3SZo+8LGHMtIyTQ==; domain=.vodacom.co.za; path=/
Set-Cookie: nlbi_2776849_2147483392=5mZ7ez+BRjupvk6+ZU49BAAAAACxj6KLVqu1zBAwGDwzNMPg; domain=.vodacom.co.za; path=/

GET https://archibus.vodacom.co.za/_Incapsula_Resource?CWUDNSAI=23&xinfo=10-115212261-0%200NNN%20RT%2816810668947 93%208%29%20q%280%20-1%20-1%20-1%29%20r

%280%20-1%29%20B15%284%2C200%2C0%29%20U18&incident_id=451000960203949962-566675017241401354&edet=15&cinfo=04000000&rpinfo=0&mth=GET
Response code: 200
Response headers:
Cache-Control: no-cache, no-store
Content-Encoding: gzip
Content-Length: 3755
Content-Security-Policy-Report-Only: default-src 'self' 'unsafe-eval' 'unsafe-hashes' 'unsafe-inline' data: blob: ; form-action 'none' data: blob: ; report-uri /csp_report
Content-Type: text/html
X-Robots-Tag: noindex
Set-Cookie: visid_incap_2776849=XzGtDabQTHuVkbHOgCNGXPUZyWUAAAAAQUIPAAAAAABzHTfqgLA/hAMNNToBRAEF; HttpOnly; expires=Sun, 09-Feb-2025 22:21:08 GMT; domain=.vodacom.co.za; path=/
Set-Cookie: nlbi_2776849=1uvTSns0kGzwA8rXZU49BAAAAABumPnVc6r7kZo+kAK6WiUr; domain=.vodacom.co.za; path=/
Set-Cookie: incap_ses_1687_2776849=ArRnARTRdWEO7PgfvG1pF/UZyWUAAAAACho9ich3SZo+8LGHMtIyTQ==; domain=.vodacom.co.za; path=/
Set-Cookie: nlbi_2776849_2147483392=5mZ7ez+BRjupvk6+ZU49BAAAAACxj6KLVqu1zBAwGDwzNMPg; domain=.vodacom.co.za; path=/

GET https://archibus.vodacom.co.za/_Incapsula_Resource?CWUDNSAI=23&xinfo=10-115214768-0%200NNN%20RT%2816810669099 96%203992%29%20q%280%20-1%20-1%200%29%20r%280%20-1%29%20B15%284%2c200%2c0%29%20U18&incident_id=451000960203949962-566690908620396554&edet=15&cinfo=04000000&rpinfo=0&mth=GET
Response code: 200
Response headers:
Cache-Control: no-cache, no-store
Content-Encoding: gzip
Content-Length: 3755
Content-Security-Policy-Report-Only: default-src 'self' 'unsafe-eval' 'unsafe-hashes' 'unsafe-inline' data: blob: ; form-action 'none' data: blob: ; report-uri /csp_report
Content-Type: text/html
X-Robots-Tag: noindex
Set-Cookie: visid_incap_2776849=XzGtDabQTHuVkbHOgCNGXPUZyWUAAAAAQUIPAAAAAABzHTfqgLA/hAMNNToBRAEF; HttpOnly; expires=Sun, 09-Feb-2025 22:21:08 GMT; domain=.vodacom.co.za; path=/
Set-Cookie: nlbi_2776849=1uvTSns0kGzwA8rXZU49BAAAAABumPnVc6r7kZo+kAK6WiUr; domain=.vodacom.co.za; path=/
Set-Cookie: incap_ses_1687_2776849=ArRnARTRdWEO7PgfvG1pF/UZyWUAAAAACho9ich3SZo+8LGHMtIyTQ==; domain=.vodacom.co.za; path=/
Set-Cookie: nlbi_2776849_2147483392=5mZ7ez+BRjupvk6+ZU49BAAAAACxj6KLVqu1zBAwGDwzNMPg; domain=.vodacom.co.za; path=/

GET https://archibus.vodacom.co.za/_Incapsula_Resource?CWUDNSAI=23&xinfo=10-126106739-0%200NNN%20RT%2816888929365204%203%29%20q%280%20-1%20-1%20-1%29%20r%280%20-1%29%20B15%284%2c200%2c0%29%20U18&incident_id=763001020386100101-604542579974543754&edet=15&cinfo=04000000&rpinfo=0&mth=GET
Response code: 200
Response headers:
Cache-Control: no-cache, no-store
Content-Encoding: gzip
Content-Length: 3755
Content-Security-Policy-Report-Only: default-src 'self' 'unsafe-eval' 'unsafe-hashes' 'unsafe-inline' data: blob: ; form-action 'none' data: blob: ; report-uri /csp_report
Content-Type: text/html
X-Robots-Tag: noindex
Set-Cookie: visid_incap_2776849=XzGtDabQTHuVkbHOgCNGXPUZyWUAAAAAQUIPAAAAAABzHTfqgLA/hAMNNToBRAEF; HttpOnly; expires=Sun, 09-Feb-2025 22:21:08 GMT; domain=.vodacom.co.za; path=/
Set-Cookie: nlbi_2776849=1uvTSns0kGzwA8rXZU49BAAAAABumPnVc6r7kZo+kAK6WiUr; domain=.vodacom.co.za; path=/
Set-Cookie: incap_ses_1687_2776849=ArRnARTRdWEO7PgfvG1pF/UZyWUAAAAACho9ich3SZo+8LGHMtIyTQ==; domain=.vodacom.co.za; path=/
Set-Cookie: nlbi_2776849_2147483392=5mZ7ez+BRjupvk6+ZU49BAAAAACxj6KLVqu1zBAwGDwzNMPg; domain=.vodacom.co.za; path=/

GET https://archibus.vodacom.co.za/_Incapsula_Resource?CWUDNSAI=23&xinfo=10-129187804-0%200NNN%20RT%2817022349388 29%203%29%20q%280%20-1%20-1%200%29%20r%280%20-1%29%20B15%284%2c200%2c0%29%20U18&incident_id=281001070577460321-698535035818023626&edet=15&cinfo=04000000&rpinfo=0&mth=GET
Response code: 200
Response headers:
Cache-Control: no-cache, no-store
Content-Encoding: gzip
Content-Length: 3757
Content-Security-Policy-Report-Only: default-src 'self' 'unsafe-eval' 'unsafe-hashes' 'unsafe-inline' data: blob: ; form-action 'none' data: blob: ; report-uri /csp_report
Content-Type: text/html
X-Robots-Tag: noindex
Set-Cookie: visid_incap_2776849=XzGtDabQTHuVkbHOgCNGXPUZyWUAAAAAQUIPAAAAAABzHTfqgLA/hAMNNToBRAEF; HttpOnly; expires=Sun, 09-Feb-2025 22:21:08 GMT; domain=.vodacom.co.za; path=/
Set-Cookie: nlbi_2776849=1uvTSns0kGzwA8rXZU49BAAAAABumPnVc6r7kZo+kAK6WiUr; domain=.vodacom.co.za; path=/
Set-Cookie: incap_ses_1687_2776849=ArRnARTRdWEO7PgfvG1pF/UZyWUAAAAACho9ich3SZo+8LGHMtIyTQ==; domain=.vodacom.co.za; path=/
Set-Cookie: nlbi_2776849_2147483392=5mZ7ez+BRjupvk6+ZU49BAAAAACxj6KLVqu1zBAwGDwzNMPg; domain=.vodacom.co.za; path=/

GET https://archibus.vodacom.co.za/_Incapsula_Resource?CWUDNSAI=23&xinfo=11-111956721-0%200NNN%20RT%2816943725209 54%2015878%29%20q%280%20-1%20-1%200%29%20r%280%20-1%29%20B15%284%2C200%2C0%29%20U18&incident_id=765000070362200247-534536421231100363&edet=15&cinfo=04000000&rpinfo=0&mth=GET
Response code: 200
Response headers:
Cache-Control: no-cache, no-store
Content-Encoding: gzip
Content-Length: 3756
Content-Security-Policy-Report-Only: default-src 'self' 'unsafe-eval' 'unsafe-hashes' 'unsafe-inline' data: blob: ; form-action 'none' data: blob: ; report-uri /csp_report
Content-Type: text/html
X-Robots-Tag: noindex
Set-Cookie: visid_incap_2776849=XzGtDabQTHuVkbHOgCNGXPUZyWUAAAAAQUIPAAAAAABzHTfqgLA/hAMNNToBRAEF; HttpOnly; expires=Sun, 09-Feb-2025 22:21:08 GMT; domain=.vodacom.co.za; path=/
Set-Cookie: nlbi_2776849=1uvTSns0kGzwA8rXZU49BAAAAABumPnVc6r7kZo+kAK6WiUr; domain=.vodacom.co.za; path=/
Set-Cookie: incap_ses_1687_2776849=ArRnARTRdWEO7PgfvG1pF/UZyWUAAAAACho9ich3SZo+8LGHMtIyTQ==; domain=.vodacom.co.za; path=/
Set-Cookie: nlbi_2776849_2147483392=5mZ7ez+BRjupvk6+ZU49BAAAAACxj6KLVqu1zBAwGDwzNMPg; domain=.vodacom.co.za; path=/

GET https://archibus.vodacom.co.za/_Incapsula_Resource?CWUDNSAI=23&xinfo=11-124742921-0%200NNN%20RT%2816919539417 046%202308%29%20q%280%20-1%20-1%200%29%20r%280%20-1%29%20B15%284%2C200%2C0%29%20U18&incident_id=128000730324386403-607342817005539915&edet=15&cinfo=04000000&rpinfo=0&mth=GET
Response code: 200
Response headers:
Cache-Control: no-cache, no-store
Content-Encoding: gzip

Content-Length: 3754
Content-Security-Policy-Report-Only: default-src 'self' 'unsafe-eval' 'unsafe-hashes' 'unsafe-inline' data: blob: ; form-action 'none' data: blob: ; report-uri /csp_report
Content-Type: text/html
X-Robots-Tag: noindex
Set-Cookie: visid_incap_2776849=XzGtDabQTHuVkbHOgCNGXPUZyWUAAAAAQUIPAAAAAABzHTfqgLA/hAMNNToBRAEF; HttpOnly; expires=Sun, 09-Feb-2025 22:21:08 GMT; domain=.vodacom.co.za; path=/
Set-Cookie: nlbi_2776849=1uvTSns0kGzwA8rXZU49BAAAAABumPnVc6r7kZo+kAK6WiUr; domain=.vodacom.co.za; path=/
Set-Cookie: incap_ses_1687_2776849=ArRnARTRdWEO7PgfvG1pF/UZyWUAAAAACho9ich3SZo+8LGHMtIyTQ==; domain=.vodacom.co.za; path=/
Set-Cookie: nlbi_2776849_2147483392=5mZ7ez+BRjupvk6+ZU49BAAAAACxj6KLVqu1zBAwGDwzNMPg; domain=.vodacom.co.za; path=/

GET https://archibus.vodacom.co.za/_Incapsula_Resource?CWUDNSAI=23&xinfo=52-10807422-0%200NNN%20RT%281705258955714%2016035%29%20q%280%20-1%20-1%201%29%20r%280%20-1%29%20B15%284%2C200%2C0%29%20U18&incident_id=168600004022514258 1-6184636094178949 2&edet=15&cinfo=04000000&rpinfo=0&mth=GET
Response code: 200
Response headers:
Cache-Control: no-cache, no-store
Content-Encoding: gzip
Content-Length: 3756
Content-Security-Policy-Report-Only: default-src 'self' 'unsafe-eval' 'unsafe-hashes' 'unsafe-inline' data: blob: ; form-action 'none' data: blob: ; report-uri /csp_report
Content-Type: text/html
X-Robots-Tag: noindex
Set-Cookie: visid_incap_2776849=XzGtDabQTHuVkbHOgCNGXPUZyWUAAAAAQUIPAAAAAABzHTfqgLA/hAMNNToBRAEF; HttpOnly; expires=Sun, 09-Feb-2025 22:21:08 GMT; domain=.vodacom.co.za; path=/
Set-Cookie: nlbi_2776849=1uvTSns0kGzwA8rXZU49BAAAAABumPnVc6r7kZo+kAK6WiUr; domain=.vodacom.co.za; path=/
Set-Cookie: incap_ses_1687_2776849=ArRnARTRdWEO7PgfvG1pF/UZyWUAAAAACho9ich3SZo+8LGHMtIyTQ==; domain=.vodacom.co.za; path=/
Set-Cookie: nlbi_2776849_2147483392=5mZ7ez+BRjupvk6+ZU49BAAAAACxj6KLVqu1zBAwGDwzNMPg; domain=.vodacom.co.za; path=/

150277 Cookie without SameSite attribute (1)

150277 Cookie without SameSite attribute *archibus.vodacom.co.za:443/fpr/index.as*

Finding #	10510207	**Severity**	Information Gathered - Level 1
Unique #	572d5abf-616e-41ad-ab34-5a137c38e48f		
Group	Security Weaknesses		
CWE	CWE-16, CWE-1032	**Detection Date**	11 Feb 2024 21:02 GMT+0200
OWASP	A5 Security Misconfiguration		
WASC	-		

Details

Threat
The cookies listed in the Results section are missing the SameSite attribute.

Impact
The SameSite cookie attribute is an effective countermeasure against cross-site request forgery (CSRF) attacks. Note that a missing SameSite attribute does not mean the web application is automatically vulnerable to CSRF. The scanner will report QID 150071 if a CSRF vulnerability is detected.

Solution
Consider adding the SameSite attribute to the cookie(s) listed.

More information:
DZone article
OWASP CSRF Prevention Cheat Sheet

Results

Total cookies: 4
incap_ses_1687_2776849=ArRnARTRdWEO7PgfvG1pF/UZyWUAAAAACho9ich3SZo+8LGHMtIyTQ==; path=/; domain=.vodacom.co.za | First set at URL: https://archibus.vodacom.co.za/fpr/index.asp
nlbi_2776849=1uvTSns0kGzwA8rXZU49BAAAAABumPnVc6r7kZo+kAK6WiUr; path=/; domain=.vodacom.co.za | First set at URL: https://archibus.vodacom.co.za/fpr/index.asp
nlbi_2776849_2147483392=a6JeKHL+xgNWhQdiZU49BAAAAABtrQ53JjbMXz9smE8uFxJx; path=/; domain=.vodacom.co.za | First set at URL: https://archibus.vodacom.co.za/fpr/index.asp
visid_incap_2776849=XzGtDabQTHuVkbHOgCNGXPUZyWUAAAAAQUIPAAAAAABzHTfqgLA/hAMNNToBRAEF; expires=Sun Feb 9 22:21:08 2025; path=/; domain=.vodacom.co.za; max-age=31459898; httponly | First set at URL: https://archibus.vodacom.co.za/fpr/index.asp

WAS Web Application Report

Appendix

Web Application Details

archibus.vodacom.co.za/

Name	archibus.vodacom.co.za/
ID	98210218
URL	https://archibus.vodacom.co.za/
Owner	Janardhan Reddy Gangireddy (vdafn5ag4)
Scope	Limit to URL hostname
Tags	ZA_WAS_EXT
Custom Attributes	-

archibus.vodacom.co.za/archibus/

Name	archibus.vodacom.co.za/archibus/
ID	98210219
URL	https://archibus.vodacom.co.za/archibus/
Owner	Janardhan Reddy Gangireddy (vdafn5ag4)
Scope	Limit to URL hostname
Tags	ZA_WAS_EXT
Custom Attributes	-

archibus.vodacom.co.za:443/fpr/index.asp

Name	archibus.vodacom.co.za:443/fpr/index.asp
ID	98210220
URL	https://archibus.vodacom.co.za:443/fpr/index.asp
Owner	Janardhan Reddy Gangireddy (vdafn5ag4)
Scope	Limit to URL hostname
Tags	ZA_WAS_EXT
Custom Attributes	-