Acunetix

Developer Report

Acunetix Security Audit

2022-11-07

Generated by Acunetix

Scan of infomswx.panasonic.cn

Scan details

Scan information	
Start time	04/11/2022, 11:34:03
Start url	https://infomswx.panasonic.cn
Host	infomswx.panasonic.cn
Scan time	37 minutes, 21 seconds
Profile	Full Scan
Responsive	True
Server OS	Unknown

Threat level

Acunetix Threat Level 2

One or more high-severity type vulnerabilities have been discovered by the scanner.A malicious user can exploit these vulnerabilities and compromise the backend database and/or deface your website.

Alerts distribution

Total alerts found	CVSS V3 Score	5
Critical	7.0-10.0	0
High	4.0-6.9	1
Medium	0.1-3.9	0
Low	0.0	4

Alerts CVSS V3 Score

Vulnerability	Overall Score
Clickjacking: X-Frame-Options header	5.8
HTTP Strict Transport Security (HSTS) not implemented	0.0
Content Security Policy (CSP) not implemented	0.0
Subresource Integrity (SRI) not implemented	0.0
Web Application Firewall detected	0.0

Alerts summary

Clickjacking: X-Frame-Options header

Classification	
CVSS3	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:C/C:N/I:L/A:N Base Score: 5.8 Attack Vector: Network Attack Complexity: Low Privileges Required: None User Interaction: None Scope: Changed Confidentiality Impact: None Integrity Impact: Low Availability Impact: None
CVSS2	Base Score: 4.3 Access Vector: Network_accessible Access Complexity: Medium Authentication: None Confidentiality Impact: None Integrity Impact: Partial Availability Impact: None Exploitability: Not_defined Remediation Level: Not_defined Report Confidence: Not_defined Availability Requirement: Not_defined Collateral Damage Potential: Not_defined Confidentiality Requirement: Not_defined Integrity Requirement: Not_defined Target Distribution: Not_defined
CWE	CWE-1021

Affected items	Variation
Web Server	1

HTTP Strict Transport Security (HSTS) not implemented

Classification	
CVSS3	CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:C/C:N/I:N/A:N Base Score: 0.0 Attack Vector: Network Attack Complexity: Low Privileges Required: None User Interaction: Required Scope: Changed Confidentiality Impact: None Integrity Impact: None Availability Impact: None

CVSS2	Base Score: 0.0 Access Vector: Network_accessible Access Complexity: Low Authentication: None Confidentiality Impact: None Integrity Impact: None Availability Impact: None Exploitability: Not_defined Remediation Level: Not_defined Report Confidence: Not_defined Availability Requirement: Not_defined Collateral Damage Potential: Not_defined Confidentiality Requirement: Not_defined Integrity Requirement: Not_defined Target Distribution: Not_defined
CWE	CWE-16

Affected items	Variation
Web Server	1

Content Security Policy (CSP) not implemented

Classification	
CVSS3	CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:C/C:N/I:N/A:N Base Score: 0.0 Attack Vector: Network Attack Complexity: Low Privileges Required: None User Interaction: Required Scope: Changed Confidentiality Impact: None Integrity Impact: None Availability Impact: None
CVSS2	Base Score: 0.0 Access Vector: Network_accessible Access Complexity: Low Authentication: None Confidentiality Impact: None Integrity Impact: None Availability Impact: None Exploitability: Not_defined Remediation Level: Not_defined Report Confidence: Not_defined Availability Requirement: Not_defined Collateral Damage Potential: Not_defined Confidentiality Requirement: Not_defined Integrity Requirement: Not_defined Target Distribution: Not_defined
CWE	CWE-1021

Affected items	Variation
Web Server	1

Subresource Integrity (SRI) not implemented

Classification

CVSS3	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:C/C:N/I:N/A:N Base Score: 0.0 Attack Vector: Network Attack Complexity: Low Privileges Required: None User Interaction: None Scope: Changed Confidentiality Impact: None Integrity Impact: None Availability Impact: None
CVSS2	Base Score: 0.0 Access Vector: Network_accessible Access Complexity: Low Authentication: None Confidentiality Impact: None Integrity Impact: None Availability Impact: None Exploitability: Not_defined Remediation Level: Not_defined Report Confidence: Not_defined Availability Requirement: Not_defined Collateral Damage Potential: Not_defined Confidentiality Requirement: Not_defined Integrity Requirement: Not_defined Target Distribution: Not_defined
CWE	CWE-830

Affected items	Variation
Web Server	1

Web Application Firewall detected

Classification	
CVSS3	CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:N Base Score: 0.0 Attack Vector: Network Attack Complexity: Low Privileges Required: None User Interaction: None Scope: Unchanged Confidentiality Impact: None Integrity Impact: None Availability Impact: None
CVSS2	Base Score: 0.0 Access Vector: Network_accessible Access Complexity: Low Authentication: None Confidentiality Impact: None Integrity Impact: None Availability Impact: None Exploitability: Not_defined Remediation Level: Not_defined Report Confidence: Not_defined Availability Requirement: Not_defined Collateral Damage Potential: Not_defined Confidentiality Requirement: Not_defined Integrity Requirement: Not_defined Target Distribution: Not_defined
CWE	CWE-16

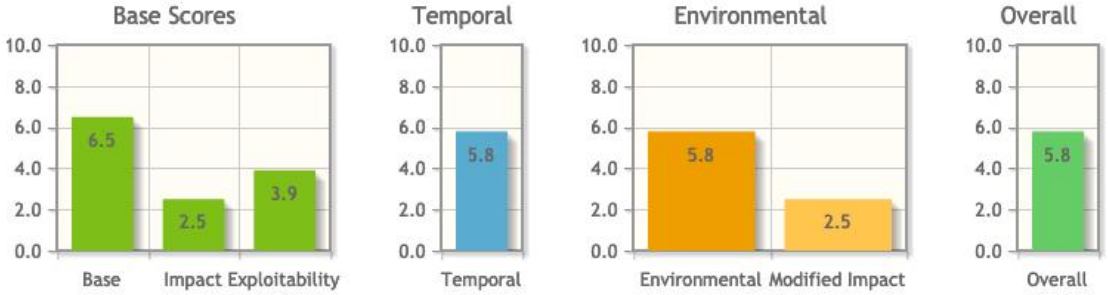
Affected items	Variation

Web Server	1

Alerts details

Clickjacking: X-Frame-Options header

Severity	**High**
CVSS V3 Score	5.8
Reported by module	/httpdata/X_Frame_Options_not_implemented.js



CVSS Base Score: 6.5
Impact Subscore: 2.5
Exploitability Subscore: 3.9
CVSS Temporal Score: 5.8
CVSS Environmental Score: 5.8
Modified Impact Subscore: 2.5
Overall CVSS Score: 5.8

Description

Clickjacking (User Interface redress attack, UI redress attack, UI redressing) is a malicious technique of tricking a Web user into clicking on something different from what the user perceives they are clicking on, thus potentially revealing confidential information or taking control of their computer while clicking on seemingly innocuous web pages.

The server did not return an **X-Frame-Options** header with the value DENY or SAMEORIGIN, which means that this website could be at risk of a clickjacking attack. The X-Frame-Options HTTP response header can be used to indicate whether or not a browser should be allowed to render a page inside a frame or iframe. Sites can use this to avoid clickjacking attacks, by ensuring that their content is not embedded into untrusted sites.

Impact

The impact depends on the affected web application.

Recommendation

Configure your web server to include an X-Frame-Options header and a CSP header with frame-ancestors directive. Consult Web references for more information about the possible values for this header.

References

The X-Frame-Options response header (https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/X-Frame-Options)
Clickjacking (https://en.wikipedia.org/wiki/Clickjacking)
OWASP Clickjacking (https://cheatsheetseries.owasp.org/cheatsheets/Clickjacking_Defense_Cheat_Sheet.html)
Frame Buster Buster (https://stackoverflow.com/questions/958997/frame-buster-buster-buster-code-needed)

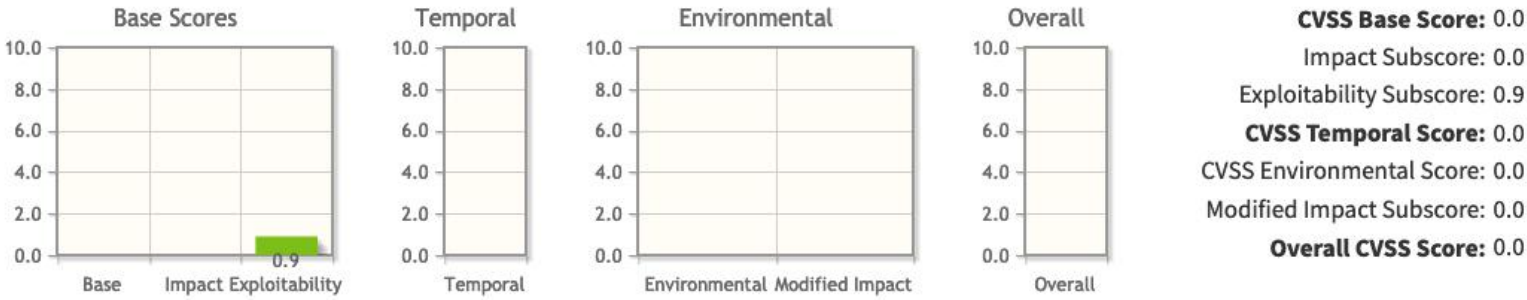
Affected items

Web Server
Details
Paths without secure XFO header: https://infomswx.panasonic.cn/ https://infomswx.panasonic.cn/index.html
Request headers

```
GET / HTTP/1.1
Referer: https://infomswx.panasonic.cn/
Cookie: _ga_VHBFZ3KY5X=GS1.1.1666194239.11.0.1666194239.60.0.0;
_ga=GA1.1.1311549070.1658972001; _gcl_au=1.1.954768786.1665198504;
__hstc=231811840.7e79e466c8eb6fac28012738507057df.1665198505434.1666174500855.16661865818
37.3; hubspotutk=7e79e466c8eb6fac28012738507057df;
JSESSIONID=0A039F1C3C4D789DE985829876F5D769;
acw_tc=0bca31c21667532540553475 2e29098b190913c74f86bcfcd6954d59392282
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip,deflate,br
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like
Gecko) Chrome/103.0.5060.114 Safari/537.36
Host: infomswx.panasonic.cn
Connection: Keep-alive
RC-Token:
eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJzdWIiOiJ0aGlzIGlzIENvbW1vbiB0b2tlbiIsImF1ZCI6IkNv
bW1vblN0YXIiLCJpc3MiOiJDb21tb25Qcm9qZWN0IiwiZXhwIjoxNjY3NTM1NjUwLCJ1c2VySWQiOiIxMDI0NjE5N
Dg1MTExMjU1MDQwIiwiaWF0IjoxNjY3NTI4NDUwfQ.oCaRKWbnQvbAart5XucxkoH2UJ6F7Kh2xsYwEPSbsuE
MVVM-Key: 1667532578744
```

HTTP Strict Transport Security (HSTS) not implemented

Severity	**Low**
CVSS V3 Score	0.0
Reported by module	/httpdata/HSTS_not_implemented.js



Description

HTTP Strict Transport Security (HSTS) tells a browser that a web site is only accessable using HTTPS. It was detected that your web application doesn't implement HTTP Strict Transport Security (HSTS) as the Strict Transport Security header is missing from the response.

Impact

HSTS can be used to prevent and/or mitigate some types of man-in-the-middle (MitM) attacks

Recommendation

It's recommended to implement HTTP Strict Transport Security (HSTS) into your web application. Consult web references for more information

References

hstspreload.org (https://hstspreload.org/)
Strict-Transport-Security (https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/Strict-Transport-Security)

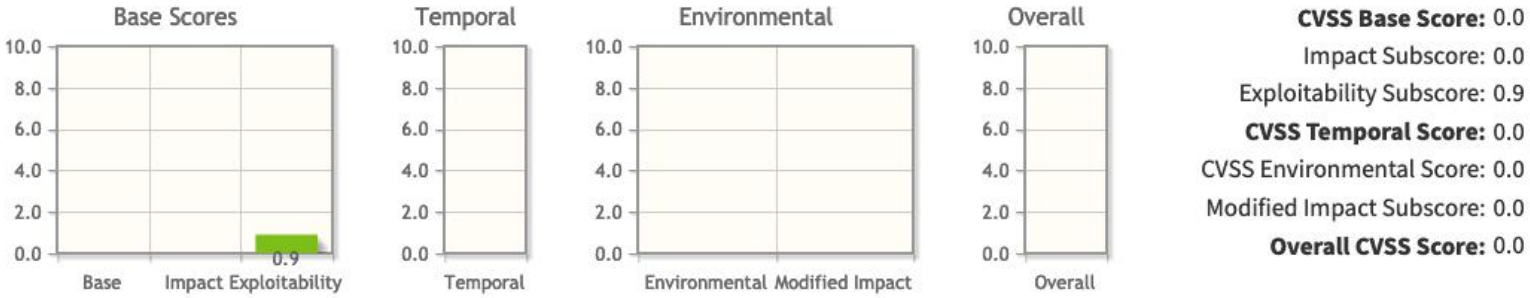
Affected items

Web Server
Details
URLs where HSTS is not enabled: https://infomswx.panasonic.cn/ https://infomswx.panasonic.cn/index.html
Request headers

```
GET / HTTP/1.1
Referer: https://infomswx.panasonic.cn/
Cookie: _ga_VHBFZ3KY5X=GS1.1.1666194239.11.0.1666194239.60.0.0;
_ga=GA1.1.1311549070.1658972001; _gcl_au=1.1.954768786.1665198504;
__hstc=231811840.7e79e466c8eb6fac28012738507057df.1665198505434.1666174500855.16661865818
37.3; hubspotutk=7e79e466c8eb6fac28012738507057df;
JSESSIONID=0A039F1C3C4D789DE985829876F5D769;
acw_tc=0bca31c21667532540553475 2e29098b190913c74f86bcfcd6954d59392282
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip,deflate,br
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like
Gecko) Chrome/103.0.5060.114 Safari/537.36
Host: infomswx.panasonic.cn
Connection: Keep-alive
RC-Token:
eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJzdWIiOiJ0aGlzIGlzIENvbW1vbiB0b2tlbiIsImF1ZCI6IkNv
bW1vblN0YXIiLCJpc3MiOiJDb21tb25Qcm9qZWN0IiwiZXhwIjoxNjY3NTM1NjUwLCJ1c2VySWQiOiIxMDI0NjE5N
Dg1MTExMjU1MDQwIiwiaWF0IjoxNjY3NTI4NDUwfQ.oCaRKWbnQvbAart5XucxkoH2UJ6F7Kh2xsYwEPSbsuE
MVVM-Key: 1667532578744
```

Content Security Policy (CSP) not implemented

Severity	**Low**
CVSS V3 Score	0.0
Reported by module	/httpdata/CSP_not_implemented.js



Description

Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks, including Cross Site Scripting (XSS) and data injection attacks.

Content Security Policy (CSP) can be implemented by adding a **Content-Security-Policy** header. The value of this header

is a string containing the policy directives describing your Content Security Policy. To implement CSP, you should define lists of allowed origins for the all of the types of resources that your site utilizes. For example, if you have a simple site that needs to load scripts, stylesheets, and images hosted locally, as well as from the jQuery library from their CDN, the CSP header could look like the following:

```
Content-Security-Policy:

    default-src 'self';

    script-src 'self' https://code.jquery.com;
```

It was detected that your web application doesn't implement Content Security Policy (CSP) as the CSP header is missing from the response. It's recommended to implement Content Security Policy (CSP) into your web application.

Impact

CSP can be used to prevent and/or mitigate attacks that involve content/code injection, such as cross-site scripting/XSS attacks, attacks that require embedding a malicious resource, attacks that involve malicious use of iframes, such as clickjacking attacks, and others.

Recommendation

It's recommended to implement Content Security Policy (CSP) into your web application. Configuring Content Security Policy involves adding the **Content-Security-Policy** HTTP header to a web page and giving it values to control resources the user agent is allowed to load for that page.

References

Content Security Policy (CSP) (https://developer.mozilla.org/en-US/docs/Web/HTTP/CSP)
Implementing Content Security Policy (https://hacks.mozilla.org/2016/02/implementing-content-security-policy/)

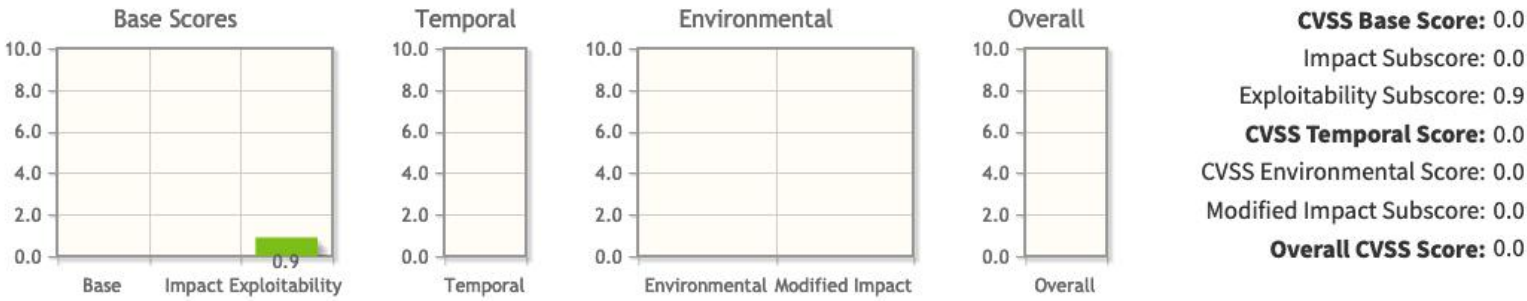
Affected items

Web Server
Details
Paths without CSP header: https://infomswx.panasonic.cn/ https://infomswx.panasonic.cn/index.html
Request headers

```
GET / HTTP/1.1
Referer: https://infomswx.panasonic.cn/
Cookie: _ga_VHBFZ3KY5X=GS1.1.1666194239.11.0.1666194239.60.0.0;
_ga=GA1.1.1311549070.1658972001; _gcl_au=1.1.954768786.1665198504;
__hstc=231811840.7e79e466c8eb6fac28012738507057df.1665198505434.1666174500855.16661865818
37.3; hubspotutk=7e79e466c8eb6fac28012738507057df;
JSESSIONID=0A039F1C3C4D789DE985829876F5D769;
acw_tc=0bca31c21667532540553475 2e29098b190913c74f86bcfcd6954d59392282
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip,deflate,br
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like
Gecko) Chrome/103.0.5060.114 Safari/537.36
Host: infomswx.panasonic.cn
Connection: Keep-alive
RC-Token:
eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJzdWIiOiJ0aGlzIGlzIENvbW1vbiB0b2tlbiIsImF1ZCI6IkNv
bW1vblN0YXIiLCJpc3MiOiJDb21tb25Qcm9qZWN0IiwiZXhwIjoxNjY3NTM1NjUwLCJ1c2VySWQiOiIxMDI0NjE5N
Dg1MTExMjU1MDQwIiwiaWF0IjoxNjY3NTI4NDUwfQ.oCaRKWbnQvbAart5XucxkoH2UJ6F7Kh2xsYwEPSbsuE
MVVM-Key: 1667532578744
```

Subresource Integrity (SRI) not implemented

Severity	**Low**
CVSS V3 Score	0.0
Reported by module	/RPA/SRI_Not_Implemented.js



Description

Subresource Integrity (SRI) is a security feature that enables browsers to verify that third-party resources they fetch (for example, from a CDN) are delivered without unexpected manipulation. It works by allowing developers to provide a cryptographic hash that a fetched file must match.

Third-party resources (such as scripts and stylesheets) can be manipulated. An attacker that has access or has hacked the hosting CDN can manipulate or replace the files. SRI allows developers to specify a base64-encoded cryptographic hash of the resource to be loaded. The integrity attribute containing the hash is then added to the <script> HTML element tag. The integrity string consists of a base64-encoded hash, followed by a prefix that depends on the hash algorithm. This prefix can either be sha256, sha384 or sha512.

The script loaded from the external URL specified in the Details section doesn't implement Subresource Integrity (SRI). It's recommended to implement Subresource Integrity (SRI) for all the scripts loaded from external hosts.

Impact

An attacker that has access or has hacked the hosting CDN can manipulate or replace the files.

Recommendation

Use the SRI Hash Generator link (from the References section) to generate a <script> element that implements Subresource Integrity (SRI).

For example, you can use the following <script> element to tell a browser that before executing the https://example.com/example-framework.js script, the browser must first compare the script to the expected hash, and verify that there's a match.

```
<script src="https://example.com/example-framework.js"
        integrity="sha384-oqVuAfXRKap7fdgcCY5uykM6+R9GqQ8K/uxy9rx7HNQlGYl1kPzQho1wx4JwY8wC    "
        crossorigin="anonymous"></script>
```

References

Subresource Integrity (https://developer.mozilla.org/en-US/docs/Web/Security/Subresource_Integrity)
SRI Hash Generator (https://www.srihash.org/)

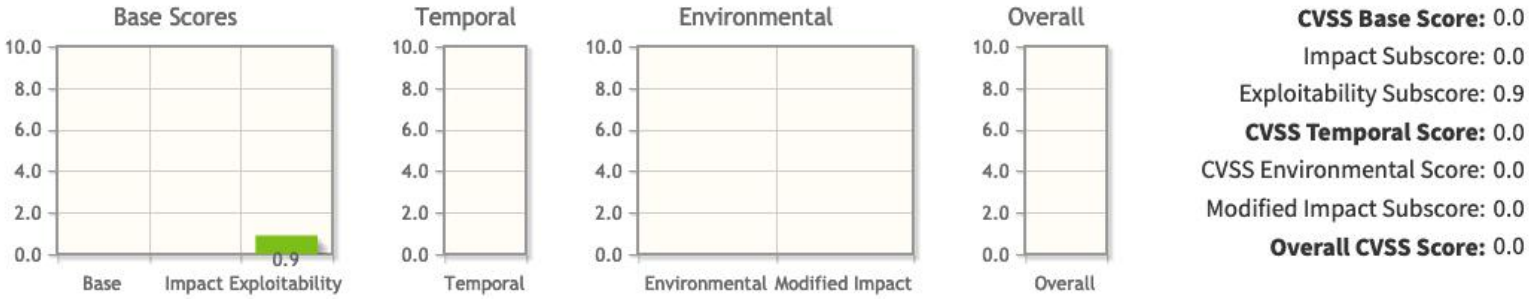
Affected items

Web Server
Details
Pages where SRI is not implemented: https://infomswx.panasonic.cn/ Script SRC: **https://webapi.amap.com/maps?v=1.4.14&key=YOUR%20KEY** https://infomswx.panasonic.cn/ Script SRC: **https://cdn.bootcdn.net/ajax/libs/vue/2.6.10/vue.min.js** https://infomswx.panasonic.cn/ Script SRC: **https://cdn.jsdelivr.net/npm/vant@2.11/lib/vant.min.js** https://infomswx.panasonic.cn/ Script SRC: **https://cdnjs.cloudflare.com/ajax/libs/moment.js/2.29.4/moment.min.js** https://infomswx.panasonic.cn/ Script SRC: **https://cdn.bootcss.com/moment.js/2.20.1/locale/zh-cn.js** https://infomswx.panasonic.cn/ Script SRC: **https://errors.aliyun.com/error.js?%0A0bca31c216675329792644662e288e**
Request headers

```
GET / HTTP/1.1
Referer: https://infomswx.panasonic.cn/
Cookie: _ga_VHBFZ3KY5X=GS1.1.1666194239.11.0.1666194239.60.0.0;
_ga=GA1.1.1311549070.1658972001; _gcl_au=1.1.954768786.1665198504;
__hstc=231811840.7e79e466c8eb6fac28012738507057df.1665198505434.1666174500855.16661865818
37.3; hubspotutk=7e79e466c8eb6fac28012738507057df;
JSESSIONID=0A039F1C3C4D789DE985829876F5D769;
acw_tc=0bca31c21667532540553475 2e29098b190913c74f86bcfcd6954d59392282
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip,deflate,br
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like
Gecko) Chrome/103.0.5060.114 Safari/537.36
Host: infomswx.panasonic.cn
Connection: Keep-alive
RC-Token:
eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJzdWIiOiJ0aGlzIGlzIENvbW1vbiB0b2tlbiIsImF1ZCI6IkNv
bW1vblN0YXIiLCJpc3MiOiJDb21tb25Qcm9qZWN0IiwiZXhwIjoxNjY3NTM1NjUwLCJ1c2VySWQiOiIxMDI0NjE5N
Dg1MTExMjU1MDQwIiwiaWF0IjoxNjY3NTI4NDUwfQ.oCaRKWbnQvbAart5XucxkoH2UJ6F7Kh2xsYwEPSbsuE
MVVM-Key: 1667532578744
```

Web Application Firewall detected

Severity	**Low**
CVSS V3 Score	0.0
Reported by module	/Scripts/PerServer/WAF_Detection.script



Description

This server is protected by an IPS (Intrusion Prevention System), IDS (Intrusion Detection System) or an WAF (Web Application Firewall). Acunetix detected this by sending various malicious payloads and detecting changes in the response code, headers and body.

Impact

You may receive incorrect/incomplete results when scanning a server protected by an IPS/IDS/WAF. Also, if the WAF detects a number of attacks coming from the scanner, the IP address can be blocked after a few attempts.

Recommendation

If possible, it's recommended to scan an internal (development) version of the web application where the WAF is not active.

Affected items

Web Server
Details

Detected Aliyundun from the response body.

Request headers

```
GET /?page=../../../../../../../../../etc/passwd%00.jpg HTTP/1.1
Cookie: _ga_VHBFZ3KY5X=GS1.1.1666194239.11.0.1666194239.60.0.0;
_ga=GA1.1.1311549070.1658972001; _gcl_au=1.1.954768786.1665198504;
__hstc=231811840.7e79e466c8eb6fac28012738507057df.1665198505434.1666174500855.16661865818
37.3; hubspotutk=7e79e466c8eb6fac28012738507057df;
JSESSIONID=0A039F1C3C4D789DE985829876F5D769;
acw_tc=0bca31c216675325405534752e29098b190913c74f86bcfcd6954d59392282;
_ga_VHBFZ3KY5X=GS1.1.1666194239.11.0.1666194239.60.0.0; _ga=GA1.1.1311549070.1658972001;
_gcl_au=1.1.954768786.1665198504;
__hstc=231811840.7e79e466c8eb6fac28012738507057df.1665198505434.1666174500855.16661865818
37.3; hubspotutk=7e79e466c8eb6fac28012738507057df;
JSESSIONID=0A039F1C3C4D789DE985829876F5D769;
acw_tc=0bca31c216675325405534752e29098b190913c74f86bcfcd6954d59392282
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip,deflate,br
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like
Gecko) Chrome/103.0.5060.114 Safari/537.36
Host: infomswx.panasonic.cn
Connection: Keep-alive
RC-Token:
eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJzdWIiOiJ0aGlzIGlzIENvbW1vbiB0b2tlbiIsImF1ZCI6IkNv
bW1vblN0YXIiLCJpc3MiOiJDb21tb25Qcm9qZWN0IiwiZXhwIjoxNjY3NTM1NjUwLCJ1c2VySWQiOiIxMDI0NjE5N
Dg1MTExMjU1MDQwIiwiaWF0IjoxNjY3NTI4NDUwfQ.oCaRKWbnQvbAart5XucxkoH2UJ6F7Kh2xsYwEPSbsuE
MVVM-Key: 1667532578744
```

Scanned items (coverage report)

https://infomswx.panasonic.cn/
https://infomswx.panasonic.cn/assets/
https://infomswx.panasonic.cn/assets/css/
https://infomswx.panasonic.cn/assets/css/app.b7e78697.css
https://infomswx.panasonic.cn/assets/css/chunk-0399453d.92036ae3.css
https://infomswx.panasonic.cn/assets/css/chunk-106da3fd.9c4cd5d1.css
https://infomswx.panasonic.cn/assets/css/chunk-1e9dc9ab.529f75e4.css
https://infomswx.panasonic.cn/assets/css/chunk-243938d0.9b0b9cb1.css
https://infomswx.panasonic.cn/assets/css/chunk-3054e366.3930669c.css
https://infomswx.panasonic.cn/assets/css/chunk-30e58f5e.a1e98dcb.css
https://infomswx.panasonic.cn/assets/css/chunk-337216cc.09da8889.css
https://infomswx.panasonic.cn/assets/css/chunk-34c9dc54.69dcca7d.css
https://infomswx.panasonic.cn/assets/css/chunk-45165b30.23e939ee.css
https://infomswx.panasonic.cn/assets/css/chunk-4d90fe79.0dd9838f.css
https://infomswx.panasonic.cn/assets/css/chunk-675eb8e5.59dd0e71.css
https://infomswx.panasonic.cn/assets/css/chunk-6c84798a.e9d5710f.css
https://infomswx.panasonic.cn/assets/css/chunk-7b135b30.191ab673.css
https://infomswx.panasonic.cn/assets/css/chunk-a8e7ed10.cf4bb6e2.css
https://infomswx.panasonic.cn/assets/css/chunk-b0d0bb58.e856a46c.css
https://infomswx.panasonic.cn/assets/css/chunk-c2341b42.51e4f046.css
https://infomswx.panasonic.cn/assets/css/chunk-e9796ae2.8949501b.css
https://infomswx.panasonic.cn/assets/css/chunk-vendors.d5543e46.css
https://infomswx.panasonic.cn/assets/fonts/
https://infomswx.panasonic.cn/assets/js/
https://infomswx.panasonic.cn/assets/js/app.ccef1784.js
https://infomswx.panasonic.cn/assets/js/chunk-0399453d.d1aaed74.js
https://infomswx.panasonic.cn/assets/js/chunk-03c6947c.b34728a1.js
https://infomswx.panasonic.cn/assets/js/chunk-106da3fd.d70c965f.js
https://infomswx.panasonic.cn/assets/js/chunk-1cb698d6.ae2ec883.js
https://infomswx.panasonic.cn/assets/js/chunk-1e9dc9ab.3c846080.js
https://infomswx.panasonic.cn/assets/js/chunk-243938d0.3686bf6b.js
https://infomswx.panasonic.cn/assets/js/chunk-2d0bd777.e6fb505d.js
https://infomswx.panasonic.cn/assets/js/chunk-3054e366.6cb133ff.js
https://infomswx.panasonic.cn/assets/js/chunk-30e58f5e.b9d8410e.js
https://infomswx.panasonic.cn/assets/js/chunk-337216cc.f61be93a.js
https://infomswx.panasonic.cn/assets/js/chunk-34c9dc54.25683f3c.js
https://infomswx.panasonic.cn/assets/js/chunk-3af80fc6.596d53a0.js
https://infomswx.panasonic.cn/assets/js/chunk-45165b30.2dcd5cb7.js
https://infomswx.panasonic.cn/assets/js/chunk-4d90fe79.af58c564.js
https://infomswx.panasonic.cn/assets/js/chunk-501fbb54.d51ec675.js
https://infomswx.panasonic.cn/assets/js/chunk-510a7da4.6bdcc4bc.js
https://infomswx.panasonic.cn/assets/js/chunk-64fe761e.e320bab7.js
https://infomswx.panasonic.cn/assets/js/chunk-675eb8e5.7539f3d8.js
https://infomswx.panasonic.cn/assets/js/chunk-6982c305.cdfaeb3f.js
https://infomswx.panasonic.cn/assets/js/chunk-6c84798a.45fb89aa.js
https://infomswx.panasonic.cn/assets/js/chunk-7b135b30.b656c5ca.js
https://infomswx.panasonic.cn/assets/js/chunk-848a3df8.d9c14317.js
https://infomswx.panasonic.cn/assets/js/chunk-a8e7ed10.94820c0e.js
https://infomswx.panasonic.cn/assets/js/chunk-b0d0bb58.7556a6ef.js
https://infomswx.panasonic.cn/assets/js/chunk-b4f9690e.aebd3051.js
https://infomswx.panasonic.cn/assets/js/chunk-c2341b42.7e32f6a1.js
https://infomswx.panasonic.cn/assets/js/chunk-e9796ae2.f834c03d.js
https://infomswx.panasonic.cn/assets/js/chunk-fe27c7d6.cb236c4a.js
https://infomswx.panasonic.cn/assets/js/chunk-vendors.31e3db7a.js
https://infomswx.panasonic.cn/build/
https://infomswx.panasonic.cn/font/
https://infomswx.panasonic.cn/index.html
https://infomswx.panasonic.cn/web/