Acunetix by Invicti

Comprehensive Report

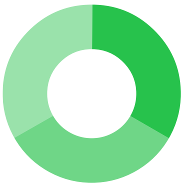
Acunetix Threat Level 3

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.

1	3	5	3
High	Medium	Low	Informational

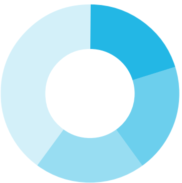
Severity	Vulnerabilities	Instances
High	1	1
Medium	3	3
Low	5	5
Informational	3	3
Total	12	12

Informational



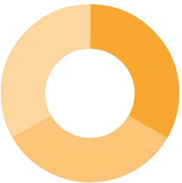
	Instances
🟩 Content Security Policy (CSP) not implemented	1
🟩 Reverse proxy detected	1
🟩 Web Application Firewall detected	1

Low Severity



	Instances
🟦 Clickjacking: X-Frame-Options header	1
🟦 Cookies with missing, inconsistent or contrad…	1
🟦 Cookies without Secure flag set	1
🟦 Others	2

Medium Severity



	Instances
🟧 TLS 1.1 enabled	1
🟧 TLS/SSL Sweet32 attack	1
🟧 TLS/SSL Weak Cipher Suites	1

High Severity

	Instances
🟥 TLS 1.0 enabled	1

Impacts

SEVERITY	IMPACT	
High	1	TLS 1.0 enabled
Medium	1	TLS 1.1 enabled
Medium	1	TLS/SSL Sweet32 attack
Medium	1	TLS/SSL Weak Cipher Suites
Low	1	Clickjacking: X-Frame-Options header
Low	1	Cookies with missing, inconsistent or contradictory properties
Low	1	Cookies without Secure flag set
Low	1	HTTP Strict Transport Security (HSTS) not implemented
Low	1	Session cookies scoped to parent domain
Informational	1	Content Security Policy (CSP) not implemented
Informational	1	Reverse proxy detected
Informational	1	Web Application Firewall detected

TLS 1.0 enabled

The web server supports encryption through TLS 1.0, which was formally deprecated in March 2021 as a result of inherent security issues. In addition, TLS 1.0 is not considered to be "strong cryptography" as defined and required by the PCI Data Security Standard 3.2(.1) when used to protect sensitive information transferred to or from web sites. According to PCI, "30 June 2018 is the deadline for disabling SSL/early TLS and implementing a more secure encryption protocol – TLS 1.1 or higher (TLS v1.2 is strongly encouraged) in order to meet the PCI Data Security Standard (PCI DSS) for safeguarding payment data.

Impact

An attacker may be able to exploit this problem to conduct man-in-the-middle attacks and decrypt communications between the affected service and clients.

---

https://cc.fsoft.com.vn/ Confidence: 100%

The SSL server (port: 443) encrypts traffic using TLSv1.0.

Recommendation

It is recommended to disable TLS 1.0 and replace it with TLS 1.2 or higher.

References

RFC 8996: Deprecating TLS 1.0 and TLS 1.1
https://tools.ietf.org/html/rfc8996

Are You Ready for 30 June 2018? Saying Goodbye to SSL/early TLS
https://blog.pcisecuritystandards.org/are-you-ready-for-30-june-2018-sayin-goodbye-to-ssl-early-tls

PCI 3.1 and TLS 1.2 (Cloudflare Support)
https://support.cloudflare.com/hc/en-us/articles/205043158-PCI-3-1-and-TLS-1-2

TLS 1.1 enabled

The web server supports encryption through TLS 1.1, which was formally deprecated in March 2021 as a result of inherent security issues. When aiming for Payment Card Industry (PCI) Data Security Standard (DSS) compliance, it is recommended to use TLS 1.2 or higher instead. According to PCI, "30 June 2018 is the deadline for disabling SSL/early TLS and implementing a more secure encryption protocol – TLS 1.1 or higher (TLS v1.2 is strongly encouraged) in order to meet the PCI Data Security Standard (PCI DSS) for safeguarding payment data.

Impact

An attacker may be able to exploit this problem to conduct man-in-the-middle attacks and decrypt communications between the affected service and clients.

---

https://cc.fsoft.com.vn/ Confidence: 100%

The SSL server (port: 443) encrypts traffic using TLSv1.1.

Recommendation

It is recommended to disable TLS 1.1 and replace it with TLS 1.2 or higher.

References

RFC 8996: Deprecating TLS 1.0 and TLS 1.1
https://tools.ietf.org/html/rfc8996

Are You Ready for 30 June 2018? Saying Goodbye to SSL/early TLS
https://blog.pcisecuritystandards.org/are-you-ready-for-30-june-2018-sayin-goodbye-to-ssl-early-tls

PCI 3.1 and TLS 1.2 (Cloudflare Support)
https://support.cloudflare.com/hc/en-us/articles/205043158-PCI-3-1-and-TLS-1-2

TLS/SSL Sweet32 attack

The Sweet32 attack is a SSL/TLS vulnerability that allows attackers to compromise HTTPS connections using 64-bit block ciphers.

Impact

An attacker may intercept HTTPS connections between vulnerable clients and servers.

---

https://cc.fsoft.com.vn/

Cipher suites susceptible to Sweet32 attack (TLS1.0 on port 443):

- TLS_RSA_WITH_3DES_EDE_CBC_SHA

Recommendation

Reconfigure the affected SSL/TLS server to disable support for obsolete 64-bit block ciphers.

References

Sweet32: Birthday attacks on 64-bit block ciphers in TLS and OpenVPN
https://sweet32.info/

TLS/SSL Weak Cipher Suites

The remote host supports TLS/SSL cipher suites with weak or insecure properties.

Impact

https://cc.fsoft.com.vn/

Weak TLS/SSL Cipher Suites: (offered via TLS1.0 on port 443):

- TLS_RSA_WITH_3DES_EDE_CBC_SHA (Medium strength encryption algorithm (3DES).)

Recommendation

Reconfigure the affected application to avoid use of weak cipher suites.

References

OWASP: TLS Cipher String Cheat Sheet
https://cheatsheetseries.owasp.org/cheatsheets/TLS_Cipher_String_Cheat_Sheet.html

OWASP: Transport Layer Protection Cheat Sheet
https://cheatsheetseries.owasp.org/cheatsheets/Transport_Layer_Protection_Cheat_Sheet.html

Mozilla: TLS Cipher Suite Recommendations
https://wiki.mozilla.org/Security/Server_Side_TLS

SSLlabs: SSL and TLS Deployment Best Practices
https://github.com/ssllabs/research/wiki/SSL-and-TLS-Deployment-Best-Practices

RFC 9155: Deprecating MD5 and SHA-1 Signature Hashes in TLS 1.2 and DTLS 1.2
https://datatracker.ietf.org/doc/html/rfc9155

Clickjacking: X-Frame-Options header

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.

https://cc.fsoft.com.vn/

Paths without secure XFO header:

- https://cc.fsoft.com.vn/backup/

Request

```
GET /backup/ HTTP/1.1
Referer: https://cc.fsoft.com.vn/
Cookie: __cf_bm=BVNI.GhctqrjITVdoIN0_XV7hn1deneetyj3jvQ89.E-1672210061-0-
AZt8HEYKgc6X/6ZzZ2nujebdjfZ5L0T4H6iBG/j64K0xkq/vKMXBQGhMaWJBIe1YmTal47v7cNbRJVELIXvLewRaSjvRGChy3Jpo
P+AyjNTI; JSESSIONID_XONE_CustomerCare=EB9D3FA9EB253D79C3BE1D904C49225D
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/99.0.4844.0 Safari/537.36
Host: cc.fsoft.com.vn
Connection: Keep-alive
```

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

Cookies with missing, inconsistent or contradictory properties

At least one of the following cookies properties causes the cookie to be invalid or incompatible with either a different property of the same cookie, of with the environment the cookie is being used in. Although this is not a vulnerability in itself, it will likely lead to unexpected behavior by the application, which in turn may cause secondary security issues.

Impact

Cookies will not be stored, or submitted, by web browsers.

---

https://cc.fsoft.com.vn/ Verified

List of cookies with missing, inconsistent or contradictory properties:

- https://cc.fsoft.com.vn/CustomerCare/

  Cookie was set with:

  ```
  Set-Cookie: JSESSIONID_XONE_CustomerCare=EB9D3FA9EB253D79C3BE1D904C49225D;
  Domain=.fsoft.com.vn; Path=/; HttpOnly
  ```

  This cookie has the following issues:

```
- Cookie without SameSite attribute.
When cookies lack the SameSite attribute, Web browsers may apply different and
sometimes unexpected defaults. It is therefore recommended to add a SameSite
attribute with an appropriate value of either "Strict", "Lax", or "None".
```

- https://cc.fsoft.com.vn/CustomerCare/

  Cookie was set with:

  ```
  Set-Cookie: OAuth_Token_Request_State=a53a7db1-6100-4b62-84b5-1ff15d7b0c42;
  Version=1; HttpOnly
  ```

  This cookie has the following issues:

  ```
  - Cookie without SameSite attribute.
  When cookies lack the SameSite attribute, Web browsers may apply different and
  sometimes unexpected defaults. It is therefore recommended to add a SameSite
  attribute with an appropriate value of either "Strict", "Lax", or "None".
  ```

- https://cc.fsoft.com.vn/CustomerCare/

  Cookie was set with:

  ```
  Set-Cookie: JSESSIONID_XONE_CustomerCare=51182D7E72ECFC05FBDEA571B5802A1B;
  Domain=.fsoft.com.vn; Path=/; HttpOnly
  ```

  This cookie has the following issues:

  ```
  - Cookie without SameSite attribute.
  When cookies lack the SameSite attribute, Web browsers may apply different and
  sometimes unexpected defaults. It is therefore recommended to add a SameSite
  attribute with an appropriate value of either "Strict", "Lax", or "None".
  ```

- https://cc.fsoft.com.vn/CustomerCare/

  Cookie was set with:

  ```
  Set-Cookie: OAuth_Token_Request_State=1912c343-09a2-4e30-a895-17db25ab678d;
  Version=1; HttpOnly
  ```

  This cookie has the following issues:

```
    - Cookie without SameSite attribute.
    When cookies lack the SameSite attribute, Web browsers may apply different and
    sometimes unexpected defaults. It is therefore recommended to add a SameSite
    attribute with an appropriate value of either "Strict", "Lax", or "None".
```

Request

```
GET /CustomerCare/ HTTP/1.1
Host: cc.fsoft.com.vn
accept-language: en-US
accept: */*
cookie: __cf_bm=4P9QsTRRFc5LGS13NKUqWQ00V9WYb35Q5Qy2d9bQ.Ek-1672209985-0-
ATnyWt5uCse8he52rEZZtDR8NIibLev/dYiwFqLigufFTLRGMcT57PoJNFJy9OYO8K+tRVo34bMG8EdF0sP/zPnJJUoaMPdj/v6K
MzMNsi6i
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: cors
Sec-Fetch-Dest: empty
Referer: https://cc.fsoft.com.vn/
Accept-Encoding: gzip,deflate,br
Connection: keep-alive
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/99.0.4844.0 Safari/537.36
```

Recommendation

Ensure that the cookies configuration complies with the applicable standards.

References

MDN | Set-Cookie
https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/Set-Cookie

Securing cookies with cookie prefixes
https://www.sjoerdlangkemper.nl/2017/02/09/cookie-prefixes/

Cookies: HTTP State Management Mechanism
https://tools.ietf.org/html/draft-ietf-httpbis-rfc6265bis-05

SameSite Updates - The Chromium Projects
https://www.chromium.org/updates/same-site

draft-west-first-party-cookies-07: Same-site Cookies
https://tools.ietf.org/html/draft-west-first-party-cookies-07

Cookies without Secure flag set

One or more cookies does not have the Secure flag set. When a cookie is set with the Secure flag, it instructs the browser that the cookie can only be accessed over secure SSL/TLS channels. This is an important security protection for session cookies.

Impact

Cookies could be sent over unencrypted channels.

---

https://cc.fsoft.com.vn/ Verified

Cookies without Secure flag set:

- https://cc.fsoft.com.vn/CustomerCare/

```
Set-Cookie: JSESSIONID_XONE_CustomerCare=EB9D3FA9EB253D79C3BE1D904C49225D;
Domain=.fsoft.com.vn; Path=/; HttpOnly
```

- https://cc.fsoft.com.vn/CustomerCare/

```
Set-Cookie: OAuth_Token_Request_State=a53a7db1-6100-4b62-84b5-1ff15d7b0c42;
Version=1; HttpOnly
```

- https://cc.fsoft.com.vn/CustomerCare/

```
Set-Cookie: JSESSIONID_XONE_CustomerCare=51182D7E72ECFC05FBDEA571B5802A1B;
Domain=.fsoft.com.vn; Path=/; HttpOnly
```

- https://cc.fsoft.com.vn/CustomerCare/

```
Set-Cookie: OAuth_Token_Request_State=1912c343-09a2-4e30-a895-17db25ab678d;
Version=1; HttpOnly
```

Request

```
GET /CustomerCare/ HTTP/1.1
Host: cc.fsoft.com.vn
accept-language: en-US
accept: */*
cookie: __cf_bm=4P9QsTRRFc5LGS13NKUqWQ00V9WYb35Q5Qy2d9bQ.Ek-1672209985-0-
ATnyWt5uCse8he52rEZZtDR8NIibLev/dYiwFqLigufFTLRGMcT57PoJNFJy9OYO8K+tRVo34bMG8EdF0sP/zPnJJUoaMPdj/v6K
MzMNsi6i
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: cors
Sec-Fetch-Dest: empty
Referer: https://cc.fsoft.com.vn/
Accept-Encoding: gzip,deflate,br
Connection: keep-alive
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/99.0.4844.0 Safari/537.36
```

Recommendation

If possible, you should set the Secure flag for these cookies.

HTTP Strict Transport Security (HSTS) not implemented

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

https://cc.fsoft.com.vn/

URLs where HSTS is not enabled:

- https://cc.fsoft.com.vn/cdn-cgi/images/trace/jsch/nojs/
- https://cc.fsoft.com.vn/cdn-cgi/images/trace/jsch/
- https://cc.fsoft.com.vn/cdn-cgi/images/trace/
- https://cc.fsoft.com.vn/backup/

Request

```
GET /cdn-cgi/images/trace/jsch/nojs/ HTTP/1.1
Referer: https://cc.fsoft.com.vn/
```

```
Cookie: __cf_bm=_PAymRdSBBjb4WIxw.fIEmcgwKmMzjckc336keU_9EI-1672210019-0-
AWUzmja444UYLLVCdxo0el6v7woOHUYZ0cZSvoEriQqZSE0lbeO0ZQ8BTOjb9LJS0JxKepeK8WKkzNssoo2cm7TLIiegy6/dgObc
84qGCpCq; JSESSIONID_XONE_CustomerCare=EB9D3FA9EB253D79C3BE1D904C49225D
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/99.0.4844.0 Safari/537.36
Host: cc.fsoft.com.vn
Connection: Keep-alive
```

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

Session cookies scoped to parent domain

One ore more session cookies are scoped to the parent domain instead of a sub-domain. If a cookie is scoped to a parent domain, then this cookie will be accessible by the parent domain and also by any other sub-domains of the parent domain. This could lead to security problems.

Impact

None

https://cc.fsoft.com.vn/ Verified

Session cookies scoped to parent domain:

- https://cc.fsoft.com.vn/

```
Set-Cookie: __cf_bm=2TFJ9FVirwv4PP0WbNrWxEINCajmgQApOuQ0LmzBsZY-1672209915-0-
AdSJT+BOSPT9f8KPNwl1DsCOOOqBpSb7IJoIMsPexmQL7yHbVNRLLY6Y9ZNtp5Yzl0iLkUnorJir25Rcs
```

```
R2yNrYgwbgU1FLelQ6zHq1wQjbh; path=/; expires=Wed, 28-Dec-22 07:15:15 GMT;
domain=.fsoft.com.vn; HttpOnly; Secure; SameSite=None
```

- https://cc.fsoft.com.vn/CustomerCare/

```
Set-Cookie: JSESSIONID_XONE_CustomerCare=EB9D3FA9EB253D79C3BE1D904C49225D;
Domain=.fsoft.com.vn; Path=/; HttpOnly
```

- https://cc.fsoft.com.vn/CustomerCare/

```
Set-Cookie: __cf_bm=.JFWxppd.dyuvE10aX4e4BA1aLrCflN..btEd6CetUM-1672209988-0-
ASQdUbtG8E0f6TLxMaTpL9BZQgZF+WRCiEJjwgXZPYx2qRzja6NQnDwIrntDMPR9AAGXqdnKkobfY8DCv
YUyMwrQrLVte/g8ZCEXZsI/BFQv; path=/; expires=Wed, 28-Dec-22 07:16:28 GMT;
domain=.fsoft.com.vn; HttpOnly; Secure; SameSite=None
```

- https://cc.fsoft.com.vn/cdn-cgi/challenge-platform/h/g/orchestrate/jsch/v1

```
Set-Cookie: __cf_bm=_PAymRdSBBjb4WIxw.fIEmcgwKmMzjckc336keU_9EI-1672210019-0-
AWUzmja444UYLLVCdxo0el6v7woOHUYZ0cZSvoEriQqZSE0lbeO0ZQ8BTOjb9LJS0JxKepeK8WKkzNsso
o2cm7TLIiegy6/dgObc84qGCpCq; path=/; expires=Wed, 28-Dec-22 07:16:59 GMT;
domain=.fsoft.com.vn; HttpOnly; Secure; SameSite=None
```

- https://cc.fsoft.com.vn/cdn-cgi/challenge-platform/h/g/orchestrate/jsch/

```
Set-Cookie: __cf_bm=U4FINuRmvHIadJab3dCN.pGQHck9qmTcO92cZu_nwDU-1672210061-0-
ARkD9Iy2ha2SSgAaRyWyykxkNt46lwM6FlkaZrGsN5OqEwCVEhzvMwb4FgJtAP7FqWCRVwuKuPn8P65FZ
xgRgVQrUmRAgGZXxVw/PPGwrmFS; path=/; expires=Wed, 28-Dec-22 07:17:41 GMT;
domain=.fsoft.com.vn; HttpOnly; Secure; SameSite=None
```

- https://cc.fsoft.com.vn/cdn-cgi/challenge-platform/

```
Set-Cookie: __cf_bm=BVNI.GhctqrjITVdoIN0_XV7hn1deneetyj3jvQ89.E-1672210061-0-
AZt8HEYKgc6X/6ZzZ2nujebdjfZ5L0T4H6iBG/j64K0xkq/vKMXBQGhMaWJBIe1YmTal47v7cNbRJVELI
XvLewRaSjvRGChy3JpoP+AyjNTI; path=/; expires=Wed, 28-Dec-22 07:17:41 GMT;
domain=.fsoft.com.vn; HttpOnly; Secure; SameSite=None
```

- https://cc.fsoft.com.vn/backup/

```
Set-Cookie: __cf_bm=NFvJ8csMgc_k.dz83aPo81YzkW4zj4zqEu28qT7klTc-1672210239-0-
AUODekv9O7Z9jxZYFMx4R4NdYk5NXKFkXaobIitrt5TUrjMc3G81NcKAMxK2Zd3xcKTK6J5rRW0J9dR6X
eXC0sZvu6q/NeJiPHeWtktXFCcA; path=/; expires=Wed, 28-Dec-22 07:20:39 GMT;
domain=.fsoft.com.vn; HttpOnly; Secure; SameSite=None
```

- https://cc.fsoft.com.vn/cdn-cgi/challenge-platform/h/g/cv/result/78085cee18792108

```
Set-Cookie: __cf_bm=91rSSc.AUQ4loQRcNxCTPYK8zCGUDYc1BojPZfj5Pfs-1672210248-0-
AVXipOjztmEetj5lCa8AJ6VDEd1nPOZMcn7yvz1T+3SpPDf/X4Y6mrwKdpjABV8ER/zu3VWLhLNAhVoDo
6TxgrOAGUjXx6LBmaAKu4cC55Cw2b9yKNaDHAyJV1WSfEbsIgbFIMoIOXXV/9mwIWudrQc=; path=/;
expires=Wed, 28-Dec-22 07:20:48 GMT; domain=.fsoft.com.vn; HttpOnly; Secure;
SameSite=None
```

- https://cc.fsoft.com.vn/cdn-cgi/challenge-platform/h/g/scripts/alpha/

```
Set-Cookie: __cf_bm=u4AKew1jv8wz8JTpeBUSVpVaQK.Rvv_zd7Xu16NIjBc-1672210631-0-
AYbKB3w7hvz7JoTqMyyjMtG8kGY/ylSXiLtzga45yaydFRYtfsHCOH6WCtfA1UUwMZRLL8Wz6DOXj3P0P
FG/hK/eDuxgS8ZUz480PgaT+0An; path=/; expires=Wed, 28-Dec-22 07:27:11 GMT;
domain=.fsoft.com.vn; HttpOnly; Secure; SameSite=None
```

- https://cc.fsoft.com.vn/cdn-cgi/challenge-platform/h/g/cv/result/

```
Set-Cookie: __cf_bm=SGl3.ZX7GxiFPdbasU.DVy_tooNsOSlmFqfFlwmemfQ-1672210631-0-
AXx3KunbLDB9fBTXKaA/5ySH8DWxwQaaS1pkSHdc/Krz7VugxVGRTsa1oN6MwJu8KPhTCpxD4qP7cD1N2
fkTxkEdSDfgyQqmkur5ngLq6LQM; path=/; expires=Wed, 28-Dec-22 07:27:11 GMT;
domain=.fsoft.com.vn; HttpOnly; Secure; SameSite=None
```

- https://cc.fsoft.com.vn/cdn-cgi/challenge-platform/h/g/scripts/

```
Set-Cookie: __cf_bm=8B9kFte1.cmiwuqLkLGlItOgmnVA8wjKKsjP_isBQuM-1672210631-0-
AYS+PPIlCB03H7p8v2heM3+UG/dJkSf0Tt5JDpX87zaCgbLJ8PZX2lbW7rl8jwioG6ikwDrefoomNeoGp
EUVTFd3A5d/hQ74IBDcUHUdkDaS; path=/; expires=Wed, 28-Dec-22 07:27:11 GMT;
domain=.fsoft.com.vn; HttpOnly; Secure; SameSite=None
```

- https://cc.fsoft.com.vn/

```
Set-Cookie: __cf_bm=R2x4VSwm7OpOEA2SkIYhPSbmznU.sB2CIcicIQMtDPE-1672211105-0-
AWOqvnr0FoWpZ/cZDXZJvTkB4cXFZiV7JubxqYPS+H+4MfAmIs6LvkfEvXEQTmu8NPbiu3MNVULvpWM61
```

```
cyWdSBy419gAHPbHJsmPFkigcNn; path=/; expires=Wed, 28-Dec-22 07:35:05 GMT;
domain=.fsoft.com.vn; HttpOnly; Secure; SameSite=None
```

- https://cc.fsoft.com.vn/

```
Set-Cookie: __cf_bm=.v_BZygiY4U2yTAQem75AghCiH1tKrnbbcwjtoMrLrI-1672211105-0-
AYwhWRU+xhkgIWHxCQ0M6JXylc2p78xJHR7PBcTBGImQMc+0p2Xn85lxrkk20mmRttaBydGbO78C/8/YA
fPPuHMC30YDlfol09GSmJ1P7nCr; path=/; expires=Wed, 28-Dec-22 07:35:05 GMT;
domain=.fsoft.com.vn; HttpOnly; Secure; SameSite=None
```

- https://cc.fsoft.com.vn/CustomerCare/

```
Set-Cookie: JSESSIONID_XONE_CustomerCare=51182D7E72ECFC05FBDEA571B5802A1B;
Domain=.fsoft.com.vn; Path=/; HttpOnly
```

- https://cc.fsoft.com.vn/CustomerCare/

```
Set-Cookie: __cf_bm=LSNnLdav7YIvMvcFfzU2lEg5GfepjVOkgqRBbxFQ7_8-1672211105-0-
AZzEsNlekkQ6qMxC5QKYY+/87grPVIpOWKZRzgAHgV6Ux6laHO3bJQoFypNIBfYXIniKUQLETh/qW/Pgf
bLqdaU1eTzj2kJTem+mBzHKtVfi; path=/; expires=Wed, 28-Dec-22 07:35:05 GMT;
domain=.fsoft.com.vn; HttpOnly; Secure; SameSite=None
```

- https://cc.fsoft.com.vn/9231299

```
Set-Cookie: __cf_bm=l1uiW8.9F1bhO.b8uoCD_FilTZwrt231xm6dUGPli0c-1672211105-0-
AfdzIohwgOo4bwyqVWj8Y5z2LWJAYa8CfryL97MgZrPUmkx0uONNjgi+jEIi87UurBsneh7Xb4742b9gn
rTuFtU7jqbb/38LFupi24YiJ6Wx; path=/; expires=Wed, 28-Dec-22 07:35:05 GMT;
domain=.fsoft.com.vn; HttpOnly; Secure; SameSite=None
```

- https://cc.fsoft.com.vn/backup/

```
Set-Cookie: __cf_bm=AbCPDMWVsdGKqvC4dq7BrlP4BRG2twzySZv.YRvBEa8-1672211105-0-
AfVWqM2eknc65fbO4Q7W6D8Xgp2F2pblG6MhHJArU8KG9i1+Cia1RGKe+bLcA5xQO/gOnEYuacSxTRXMl
3I4llt3kUWMkP2U3mV9EiNFsW4T; path=/; expires=Wed, 28-Dec-22 07:35:05 GMT;
domain=.fsoft.com.vn; HttpOnly; Secure; SameSite=None
```

- https://cc.fsoft.com.vn/cdn-cgi/

```
Set-Cookie: __cf_bm=9zSCS.CnAgYJC4BCy53C25RmqXOzJ6gKeGoNobzAvCo-1672211105-0-
AbmASaGytZR/Lm/VXE5hyBMJUb2ofQ+PG889H2ehpR/ETBJQqlQNXEUeDW8z/iovIo8lDXb/DwDxM80+V
UCb8yhFAVY/8wnnyjOTw/yFYAqo; path=/; expires=Wed, 28-Dec-22 07:35:05 GMT;
domain=.fsoft.com.vn; HttpOnly; Secure; SameSite=None
```

- https://cc.fsoft.com.vn/cdn-cgi/challenge-platform/h/g/cv/result/7808720f5a2d0955

```
Set-Cookie: __cf_bm=9HKn0GFEmYxglq7.peoPAkh3cPZMOEaYQP2UoU5rnwk-1672211130-0-
AcL5UyWx+ytNN1O5Kk1siXW2YRUEdQyBhqelP5hxcSL9pjthMoj3hfeqSrOLDNl06lh42Kx89UPrk0Azf
TZ/3ArmrNAKPzj3sfEqQW6HWOUIJUc0zSTkyKie6CnnXbJiGEaL9+ZftORfxKWt2Erqeds=; path=/;
expires=Wed, 28-Dec-22 07:35:30 GMT; domain=.fsoft.com.vn; HttpOnly; Secure;
SameSite=None
```

- https://cc.fsoft.com.vn/cdn-cgi/challenge-platform/

```
Set-Cookie: __cf_bm=7JWLZDh9kggF4A0IknUMYihU4DjIKwBolO.bT2ZfcwA-1672211105-0-
AQWo/PqAOQ2Ojik86MqNv/bAIVYbreO6kXjRW/U02ZkP2fI8shshIO7GyI2pHF8t7JAFk+g4eppvr2ra+
6YMcPgNprxr4MEriGJneTZwigdC; path=/; expires=Wed, 28-Dec-22 07:35:05 GMT;
domain=.fsoft.com.vn; HttpOnly; Secure; SameSite=None
```

- https://cc.fsoft.com.vn/cdn-cgi/challenge-platform/h/g/cv/result/78085cee18792108

```
Set-Cookie: __cf_bm=D6XQQ0aYyemWXK3gbq0YIwSAseyeOf4zohMCuZdtRAU-1672211105-0-
ATup8Y5UOiIx8iXbbYvBf8p6uLcdbaJ9rCp0qwjRDssfnPRN52cKNlsn0kIUBOC4O97CWimwsnOtyHtnu
gZJuS3BGH1a2Y2eHaujtU12052u+WugjPnvRWgS5y7thJZQvECO7lE3V70b8juylxW50sw=; path=/;
expires=Wed, 28-Dec-22 07:35:05 GMT; domain=.fsoft.com.vn; HttpOnly; Secure;
SameSite=None
```

Request

```
GET / HTTP/1.1
Referer: https://cc.fsoft.com.vn/
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/99.0.4844.0 Safari/537.36
Host: cc.fsoft.com.vn
Connection: Keep-alive
```

Recommendation

If possible, the session cookies should be scoped strictly to a sub-domain.

Content Security Policy (CSP) not implemented

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.

https://cc.fsoft.com.vn/

Paths without CSP header:

- https://cc.fsoft.com.vn/cdn-cgi/images/trace/jsch/nojs/
- https://cc.fsoft.com.vn/cdn-cgi/images/trace/jsch/
- https://cc.fsoft.com.vn/cdn-cgi/images/trace/
- https://cc.fsoft.com.vn/backup/

Request

```
GET /cdn-cgi/images/trace/jsch/nojs/ HTTP/1.1
Referer: https://cc.fsoft.com.vn/
Cookie: __cf_bm=_PAymRdSBBjb4WIxw.fIEmcgwKmMzjckc336keU_9EI-1672210019-0-
AWUzmja444UYLLVCdxo0el6v7woOHUYZ0cZSvoEriQqZSE0lbeO0ZQ8BTOjb9LJS0JxKepeK8WKkzNssoo2cm7TLIiegy6/dgObc
84qGCpCq; JSESSIONID_XONE_CustomerCare=EB9D3FA9EB253D79C3BE1D904C49225D
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/99.0.4844.0 Safari/537.36
Host: cc.fsoft.com.vn
Connection: Keep-alive
```

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/

Reverse proxy detected

This server uses a reverse proxy, a load balancer or a CDN (Content Delivery Network) or it's hosted in a cloud provider. Acunetix detected this by sending various payloads and detecting changes in headers and body.

Impact

No impact is associated with this vulnerability.

https://cc.fsoft.com.vn/

Detected reverse proxy: CloudFlare

Request

```
GET / HTTP/1.1
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/99.0.4844.0 Safari/537.36
Host: cc.fsoft.com.vn
Connection: Keep-alive
```

Recommendation

None

Web Application Firewall detected

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.

https://cc.fsoft.com.vn/

Detected Cloudflare WAF from the headers.

Request

```
GET /9231299 HTTP/1.1
Cookie: __cf_bm=2TFJ9FVirwv4PP0WbNrWxEINCajmgQApOuQ0LmzBsZY-1672209915-0-
AdSJT+BOSPT9f8KPNwl1DsCOOOqBpSb7IJoIMsPexmQL7yHbVNRLLY6Y9ZNtp5Yzl0iLkUnorJir25RcsR2yNrYgwbgU1FLelQ6z
Hq1wQjbh
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/99.0.4844.0 Safari/537.36
Host: cc.fsoft.com.vn
Connection: Keep-alive
```

Recommendation

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

Coverage

https://cc.fsoft.com.vn/