

Cấu hình chỉnh sửa rule 941310: false positive

1. Tuning

BGT_6101_US-ASCII Malformed Encoding XSS Filter - Attack Detected_BGT-PDC

HTTP Transaction category

1. Request Timestamp: Mon Apr 18 15:08:18 2022

2. Client IP: 192.168.140.100

3. Request Method: POST

4. Request URI: /EAgentWS/services/apis/newcust

5. Request Headers Content Type: text/plain

6. Request Headers User Agent: Java/1.8.0_181

7. Response HTTP Code: 200

Alert category

1. Rule Name: US-ASCII Malformed Encoding XSS Filter - Attack Detected

2. Rule ID: 941310

3. Severity: 2

4. Core Rule Set: OWASP CRS/3.2.0

Show less

WAF Raw Log Link (Access through CSD-Portal)

https://10.100.200.217:5601/app/discover#/doc/nginx-modsec-*/nginx-modsec-2022.16?id=u3C304AB4EV0ohALiZmd

INSTRUCTION

Alert chứa@a "/apis/newcust" --> Review

This alert has nothing to ask VirusTotal

Reviewed by FIS.SRV

Suppressed

Create a ticket for tier 2

Add Help

Delete Help

1.1. Kiểm tra request.

← → ↻ 🔒 Not secure | https://10.100.200.217:5601/app/discover#/doc/nginx-modsec-*/nginx-modsec-2022.16?id=VktCO4ABnR6I5PSEBNxj

Discover

nginx-modsec-2022.16#VktCO4ABnR6I5PSEBNxj

transaction.producer.connector	modsecurity-nginx-v3.0.4
transaction.producer.modsecurity	ModSecurity v3.0.4 (Linux)
transaction.producer.secrules_engine	DetectionOnly
transaction.request.headers.Accept	text/html, image/gif, image/jpeg, *, q=.2, */*; q=.2
transaction.request.headers.Authorization	YWdlbnRpZD02NjY2NjY2Nix0aWQ9MUQ1Q0UwOUQ4QjAwNDI3Rj1GMjY1Q0VBMjg4MkJOEi=
transaction.request.headers.Connection	keep-alive
transaction.request.headers.Content-Type	text/plain
transaction.request.headers.Host	192.168.240.100:8080
transaction.request.headers.User-Agent	Java/1.8.0_181
transaction.request.http_version	1.1
transaction.request.method	POST
transaction.request.query	transid=635b2ef7a68bd&custData=%3CcustData%3E%3Cmobile%3E0963695966%3C%2Fmobile%3E%3Cstatus%3EN%3C%2F%3C%2Fstatus%3E%3CfullName%3EB%3C%3C%2FfullName%3E%3Cdob%3E19951228%3C%2Fdob%3E%3Cgender%3EM%3C%2Fgender%3E%3Cidnum%3E022095002345-20210813-VN%3C%2Fidnum%3E%3Cpassport%3E%3Cemail%3Eboyhanoi.air%40gmail.com%3C%2Femail%3E%3Caddr1%3E%3C%2Faddr1%3E%3Caddr2%3E%3C%2Faddr2%3E%3Cprovince%3E22%3C%2Fprovince%3E%3Cdistrict%3E195%3C%2Fdistrict%3E%3Cward%3EPh%3C%3C%2Fward%3E%3Cposn%3E%3Cbank%3EMB%3C%2Fbank%3E%3Cbankacct%3E6040103866007%3C%2Fbankacct%3E%3Cbankname%3EBUI%20THE%20DANG%3C%2Fbankname%3E%3C%2FcustData%3E
transaction.request.uri	/EAgentWS/services/apis/newcust

1.2. Decode URL thành text để kiểm tra dấu hiệu tấn công XSS

transid=635b2ef7a68bd&custData=%3CcustData%3E%3Cmobile%3E0963695966%3C%2Fmobile%3E%3Cstatus%3EN%3C%2Fstatus%3E%3CfullName%3EB%3C%3C%2FfullName%3E%3Cdob%3E19951228%3C%2Fdob%3E%3Cgender%3EM%3C%2Fgender%3E%3Cidnum%3E022095002345-20210813-VN%3C%2Fidnum%3E%3Cpassport%3E%3Cemail%3Eboyhanoi.air%40gmail.com%3C%2Femail%3E%3Caddr1%3E%3C%2Faddr1%3E%3Caddr2%3E%3C%2Faddr2%3E%3Cprovince%3E22%3C%2Fprovince%3E%3Cdistrict%3E195%3C%2Fdistrict%3E%3Cward%3EPh%3C%3C%2Fward%3E%3Cposn%3E%3Cbank%3EMB%3C%2Fbank%3E%3Cbankacct%3E6040103866007%3C%2Fbankacct%3E%3Cbankname%3EBUI%20THE%20DANG%3C%2Fbankname%3E%3C%2FcustData%3E

transid=635b2ef7a68bd&custData=<custData><mobile>0963695966</mobile><status>N</status><fullName>BUI THẾ ĐĂNG</fullName><dob>19951228</dob><gender>M</gender><idnum>022095002345-20210813-VN</idnum><passport></passport><email>boyhanoi.air@gmail.com</email><addr1></addr1><addr2></addr2><province>22</province><district>195</district><ward>Phường Quang Hanh</ward><post>10000</post><region>22</region><bank>MB</bank><bankacct>6040103866007</bankacct><bankname>BUI THE DANG</bankname></custData>

transid=635b2ef7a68bd&custData=<custData><mobile>0963695966</mobile><status>N</status><fullName>BUI THẾ ĐĂNG</fullName><dob>19951228</dob><gender>M</gender><idnum>022095002345-20210813-VN</idnum><passport></passport>

Sau khi kiểm tra kết luận Query an toàn không chứa ký tự dấu hiệu tấn công XSS => False positive

2. Fixing #2.1. Nguyên nhân Với rule XSS này vẫn dễ gây ra cảnh báo sai là do Query. Request có chứa các ký tự UTF-8 trong XML data của Query cụ thể là <fullName>BUI THẾ ĐĂNG</fullName> , trong rule phát hiện XSS áp dụng với US-ASCII khi thực hiện match sẽ có những ký tự đặc biệt được quy đổi thành " hoặc & dẫn đến cảnh báo kích hoạt sai.

2.2. Cấu hình chỉnh sửa rule

Tại thư mục lưu trữ rule: `rules/` Chỉnh sửa tại file : `REQUEST-941-APPLICATION-ATTACK-XSS.conf` Ở Rule id: **941310** - Trước khi sửa

```
SecRule REQUEST_COOKIES|!REQUEST_COOKIES:/__utm/|REQUEST_COOKIES_NAMES|ARGS_NAMES|ARGS|XML:/* "@rx \xbc[^\xbe]*[\xbe]|<[^\xbe]*\xbe" \
    "id:941310,\
    phase:2,\
    block,\
    capture,\
    t:none,t:urlDecodeUni,t:lowercase,t:urlDecode,t:htmlEntityDecode,t:jsDecode,\
    msg:'US-ASCII Malformed Encoding XSS Filter - Attack Detected',\
    logdata:'Matched Data: %{TX.0} found within %{MATCHED_VAR_NAME}: %{MATCHED_VAR}',\
```

- Sau khi thêm `t:utf8toUnicode`

```
SecRule REQUEST_COOKIES|!REQUEST_COOKIES:/__utm/|REQUEST_COOKIES_NAMES|ARGS_NAMES|ARGS|XML:/* "@rx \xbc[^\xbe]*[\xbe]|<[^\xbe]*\xbe" \
    "id:941310,\
    phase:2,\
    block,\
    capture,\
    t:none,t:utf8toUnicode,t:urlDecodeUni,t:lowercase,t:urlDecode,t:htmlEntityDecode,t:jsDecode,\
    msg:'US-ASCII Malformed Encoding XSS Filter - Attack Detected',\
    logdata:'Matched Data: %{TX.0} found within %{MATCHED_VAR_NAME}: %{MATCHED_VAR}'"
```

Preferences

- [github](#)
- [Modsec-NginX](#)