

Instituto Tecnológico Colonia CTC

Seguridad Informática: Todo Ofertas

Entregado como requisito para la obtención del título Analista Programador.


Alumnos: Agustín Bartel - Octavio Etchevarrén - Alex Besozzi

Tutor: Peter Fernández

Año: 2022

Snyk:

▼

 2

OctaE3/ToDoOfertas

0

C

1

H


3

M

0

L

+

 Code analysis

0

C

0

H


2


M

0

L

Tested 15 minutes ago



 TODOOFERTAS/
TODOOFERTAS.csproj

.NETFramework,Version=v4.8

0

C

1

H


1

M

0

L

Tested 2 minutes ago



Análisis de Código:

M

Open Redirect

SNYK CODE

CWE-601

SCORE
552

30

|

|

return;

31

|

var fdurlb = fdurl.split("?")[0];

32

|

if (document.location.href.indexOf(fdurlb) < 0)

33

|

{

34

|

document.location.href=fdurl;


Unsanitized input from *the document location flows* into *window.location*, where it is used as an URL to redirect the user. This may result in an Open Redirect vulnerability.


🔗


packages/Microsoft.AspNet.ScriptManager.WebForms.5.0.0/content/Scripts/WebForms/SmartNav.js

9 steps in 1 file

NEW

 Learn about this type of vulnerability and how to fix it

 Ignore

 Full details

M

Open Redirect

SNYK CODE

CWE-601

SCORE
552

30

|

|

return;

31

|

var fdurlb = fdurl.split("?")[0];

32

|

if (document.location.href.indexOf(fdurlb) < 0)

33

|

{

34

|

document.location.href=fdurl;


Unsanitized input from *the document location flows* into *window.location*, where it is used as an URL to redirect the user. This may result in an Open Redirect vulnerability.


🔗


TODOOFERTAS/Scripts/WebForms/SmartNav.js

9 steps in 1 file

NEW

 Learn about this type of vulnerability and how to fix it

 Ignore

 Full details

Vulnerabilidades:

M jQuery - Cross-site Scripting (XSS)

SCORE
701

VULNERABILITY | [CWE-79](#) | [CVE-2020-11023](#) | [CVSS 6.3](#) **MEDIUM** | [SNYK-DOTNET-JQUERY-565440](#)

Introduced through jQuery@3.4.1
Fixed in jQuery@3.5.0

Exploit maturity **MATURE**

Show less detail ^


Detailed paths and remediation

- Introduced through: project@* > jQuery@3.4.1
Fix: [Upgrade to jQuery@3.5.0](#) ?

Overview

jQuery is a nuget package provides jQuery for .NET applications.

Affected versions of this package are vulnerable to Cross-site Scripting (XSS) Passing HTML containing `<option>` elements from untrusted sources - even after sanitizing it - to one of jQuery's DOM manipulation methods (i.e. `.html()`, `.append()`, and others) may execute untrusted code.


NEW  [Learn about this type of vulnerability](#)

 Ignore  Fix this vulnerability

H Newtonsoft.Json - Insecure Defaults

SCORE
696

VULNERABILITY | [CWE-755](#) | [CVSS 7.5](#) **HIGH** | [SNYK-DOTNET-NEWTONSOFTJSON-2774678](#)

 **Insights:** This vulnerability is only applicable on systems deployed on IIS (Internet Information Services) web-server

Introduced through Newtonsoft.Json@12.0.2
Fixed in Newtonsoft.Json@13.0.1

Exploit maturity **PROOF OF CONCEPT**

Show less detail ^

Detailed paths and remediation

- Introduced through: project@* > Newtonsoft.Json@12.0.2
Fix: [Upgrade to Newtonsoft.Json@13.0.1](#) ?

Overview

Affected versions of this package are vulnerable to Insecure Defaults due to improper handling of StackOverflow exception (SOE) whenever nested expressions are being processed. Exploiting this vulnerability results in Denial Of Service (DoS), and it is exploitable when an attacker sends 5 requests that cause SOE in time frame of 5 minutes.

Note: This vulnerability is only applicable to systems deployed on IIS (Internet Information Services) web-server

 Ignore  Fix this vulnerability

Posible solución:

- Actualizar jQuery y JSON a la última versión disponible.

Burp Suite

SqlMap

```

[1.6.7.2#dev]
https://sqlmap.org

[!] legal disclaimer: Usage of sqlmap for attacking targets without prior mutual consent is illegal. It is the end user's responsibility to obey all applicable local, state and federal laws. Developers assume no liability and are not responsible for any misuse or damage caused by this program

[*] starting @ 18:17:11 /2022-08-17/

[18:17:12] [WARNING] you've provided target URL without any GET parameters (e.g. 'http://www.site.com/article.php?id=1') and without providing any POST parameters through option '--data'
do you want to try URI injections in the target URL itself? [Y/n/q] y
[18:17:20] [INFO] testing connection to the target URL
[18:17:20] [INFO] checking if the target is protected by some kind of WAF/IPS
[18:17:20] [CRITICAL] WAF/IPS identified as 'ASP.NET RequestValidationMode (Microsoft)'
are you sure that you want to continue with further target testing? [Y/n] y
[18:17:21] [WARNING] please consider usage of tamper scripts (option '--tamper')
[18:17:21] [INFO] testing if the target URL content is stable
[18:17:22] [WARNING] target URL content is not stable (i.e. content differs). sqlmap will base the page comparison on a sequence matcher. If no dynamic nor injectable parameters are detected, or in case of junk results, refer to user's manual paragraph 'Page comparison'
how do you want to proceed? [(C)ontinue/(s)tring/(r)egex/(q)uit] c
[18:17:27] [INFO] testing if URI parameter '#1' is dynamic
[18:17:27] [WARNING] URI parameter '#1' does not appear to be dynamic
[18:17:27] [WARNING] heuristic (basic) test shows that URI parameter '#1' might not be injectable
[18:17:28] [INFO] testing for SQL injection on URI parameter '#1'
[18:17:28] [INFO] testing 'AND boolean-based blind - WHERE or HAVING clause'
[18:17:28] [WARNING] reflective value(s) found and filtering out
[18:17:28] [INFO] testing 'Boolean-based blind - Parameter replace (original value)'
[18:17:28] [INFO] testing 'MySQL >= 5.1 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (EXTRACTVALUE)'
[18:17:28] [INFO] testing 'PostgreSQL AND error-based - WHERE or HAVING clause'
[18:17:28] [INFO] testing 'Microsoft SQL Server/Sybase AND error-based - WHERE or HAVING clause (IN)'
[18:17:29] [INFO] testing 'Oracle AND error-based - WHERE or HAVING clause (XMLType)'
[18:17:29] [INFO] testing 'Generic inline queries'
[18:17:29] [INFO] testing 'PostgreSQL > 8.1 stacked queries (comment)'
[18:17:29] [INFO] testing 'Microsoft SQL Server/Sybase stacked queries (comment)'
[18:17:29] [INFO] testing 'Oracle stacked queries (DBMS_PIPE.RECEIVE_MESSAGE - comment)'
[18:17:29] [INFO] testing 'MySQL >= 5.0.12 AND time-based blind (query SLEEP)'
[18:17:29] [INFO] testing 'PostgreSQL > 8.1 AND time-based blind'
[18:17:29] [INFO] testing 'Microsoft SQL Server/Sybase time-based blind (IF)'
[18:17:29] [INFO] testing 'Oracle AND time-based blind'
it is recommended to perform only basic UNION tests if there is not at least one other (potential) technique found. Do you want to reduce the number of requests? [Y/n] y
[18:17:33] [INFO] testing 'Generic UNION query (NULL) - 1 to 10 columns'
[18:17:34] [WARNING] URI parameter '#1' does not seem to be injectable
[18:17:34] [CRITICAL] all tested parameters do not appear to be injectable. Try to increase values for '--level'/'--risk' options if you wish to perform more tests. If you suspect that there is some kind of protection mechanism involved (e.g. WAF) maybe you could try to use option '--tamper' (e.g. '--tamper-space2comment') and/or switch '--random-agent'
[18:17:34] [WARNING] HTTP error codes detected during run:
400 (Bad Request) - 20 times, 404 (Not Found) - 53 times, 500 (Internal Server Error) - 1 times

[*] ending @ 18:17:34 /2022-08-17/

E:\BurpSuiteCommunity>
```

Sql Injection

Login Administrador

Cédula

12345678

Contraseña

.....

Ingresar

Datos incorrectos

Datos ingresados:

Cédula: 12345678

Contraseña: SELECT cedula, password FROM Usuario WHERE cedula = 12345678 OR '1'='1'

```
1 POST /Presentacion/wfrmLogin HTTP/2
2 Host: localhost:44327
3 Content-Length: 778
4 Cache-Control: max-age=0
5 Sec-Ch-Ua: "Chromium";v="103", ".Not/A)Brand";v="99"
6 Sec-Ch-Ua-Mobile: ?0
7 Sec-Ch-Ua-Platform: "Windows"
8 Upgrade-Insecure-Requests: 1
9 Origin: https://localhost:44327
10 Content-Type: application/x-www-form-urlencoded
11 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/103.0.5060.134 Safari/537.36
12 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9
13 Sec-Fetch-Site: same-origin
14 Sec-Fetch-Mode: navigate
15 Sec-Fetch-User: ?1
16 Sec-Fetch-Dest: document
17 Referer: https://localhost:44327/Presentacion/wfrmLogin
18 Accept-Encoding: gzip, deflate
19 Accept-Language: es-419,es;q=0.9
20
21 EVENTTARGET=&_EVENTARGUMENT=&_VIEWSTATE=|
8Qb35zKAUvFZuckPSN4yqm1lCyp2QbH92QFQ6zg6bLcAsAbvvayovm8R1tUSDd42FVHkojUCE1sXSa60UdxfInd6KrvhlUhfqM1vSLBDFG10W7762GA54wFrreXDXjGUld2mFgNVz7Togo02Zcoa2ZKow42BdF293n5Zwu7Xf24aJ43eN627rLkt217C2hSqi
2UIR5V3SVL42Fpbln4L7Q42FvVqc5g2biSHimEXTtOTJYkHS0AyDh42FBdi2g242BRJIqqYv6_VIEWSTATEGENERATOR=AD780466&_EVENTVALIDATION=
mogRA42Bsy2LLAP42F0S096642Bqm0QDKW8suqIjIDuSuQ0FUZWRGEkzh9UmA2Wx8blfBpFK42BhI3TIPqxAvBzlwFppiObCoa04cxmxd5bpvmlNh5w42FHDnSC2w42BXHPxJSp1V6tkjhEXlHxNjYyda2mFtYs2TW1Q2E42FtJKYUGV92hFsYDGuYVe58pBHI42
FINRfmxKzcIkcactl00424MainContent424txtCedula=12345678&ctl00424MainContent424txtPassword=SELECT+cedula+password+FROM+Usuario+WHERE+cedula+3D+12345678+OR+427142743D4271427&
ctl00424MainContent424btnIniciarSesion=Ingresar
```

Sonar Cloud:



- Comprobando el detalle de los distintos bugs y advertencias de seguridad, encontramos que todos están relacionados con la librería jQuery y la biblioteca Bootstrap que se instalan por defecto al crear un proyecto ASP.NET.

Posible solución:

- Actualizar jQuery y Bootstrap a la última versión disponible.

Aclaraciones:

- Somos conscientes que no debería haber un formulario que sea fácilmente accesible para registrar administradores. Lo incluimos para que el usuario que pruebe el programa pueda acceder a las distintas funciones que este tipo de usuarios tiene. Por ejemplo: Ingresar, eliminar o modificar promociones.