‘

- Cross Site Scripting

Web Attacks

(XSS, PHPSESSID,)

Splunk Incident ID: b28e8a68-ad82-4ab6-999f-67e95c3cba46
Description:
summery:
attacker used ADOBE MUSE servise on amazon server with alert popup window that write "EXPRESSION "to attack the target.

Complite: on Addetional TItle

Score Exceeded :

Score Exceeded (Total Inbound Score: 15 - SQLI=0,XSS=15,RFI=0,LFI=0,RCE=0,PHPI=0,HTTP=0,SESS=0):

URL:
Encoded log: - GET /js/jquery-1.8.3.min.js
Decoded log: -

ON BODY :
Encoded code inject:
Referer: http://oldsystem.cydeosec.com/search.php?searchdata=%3Cstyle%3E*
{x:%EF%BD%85%EF%BD%98%EF%BD%90%EF%BD%92%EF%BD%85%EF%BD%93%EF%BD%93
%EF%BD%89%EF%BD%8F%EF%BD%8E(javascript:alert(1))}

%3C/style%3E&search=Accept-Encoding:%20gzip,%20deflate%20Accept-Language:%20tr-TR,tr;q=0.9,en-US;q=0.8,en;q=0.7%20Cookie:%20PHPSESSID=u1j76fmkbd0010si77f5aig0ol

Decoded code inject:

Referer: http://oldsystem.cydeosec.com/search.php?searchdata=<style>*
{x:ｅｘｐｒｅｓｓｉｏｎ(javascript:alert(1))}

</style>&search=Accept-Encoding: gzip, deflate Accept-Language: tr-TR,tr;q=0.9,en-US;q=0.8,en;q=0.7 Cookie: PHPSESSID=u1j76fmkbd0010si77f5aig0ol

Attacker Info:

IP: 35.90.52.181

User Agent:: Mozilla/5.0 , Gecko/20100101

Browser Name: - Firefox/

Browser Version: - 109.0

OS: - (Windows NT 10.0; Win64; x64; rv:109.0) Gecko/20100101

Analyst Investigation Results:

Virus Total Result:

No security vendor flagged this IP address as malicious

Security vendors' analysis : Suspicious

[here|https://www.virustotal.com/gui/ip-address/35.90.52.181/detection
]

Communicating Files RElATION;

Security Vendors' Analysis from TAlos:

Talos Intelligence:

LOCATION DATA : Boardman, United States
REPUTATION DETAILS:
IP Reputation: Poor
Web Reputation : Unknown

EMAIL VOLUME DATA :

SPAM LEVEL : Critical

BLOCK LISTS:
BL.SPAMCOP.NET : Not Listed
CBL.ABUSEAT.ORG: Listed
PBL.SPAMHAUS.ORG: Not Listed
SBL.SPAMHAUS.ORG: Not Listed
here

Security Vendors' Analysis from SHODAN: - No results found

[here|https://www.shodan.io/search?query=35.90.52.181
]

Victim: 38.242.128.144 (cydeooldserver)
Raw Data:
[31/Oct/2023:16:42:33 +0100] ZUEgaflfzxEfl2@cmxxCxAAAAAY 35.90.52.181 49756 38.242.128.144 80
--
GET /js/jquery-1.8.3.min.js HTTP/1.1
Host: oldsystem.cydeosec.com

Connection: keep-alive
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:109.0) Gecko/20100101 Firefox/109.0
Accept: **/**
Referer: http://oldsystem.cydeosec.com/search.php?searchdata=%3Cstyle%3E*{x:%EF%BD%85%EF%BD%98%EF%BD%90%EF%BD%92%EF%BD%85%EF%BD%93%EF%BD%93%EF%BD%89%EF%BD%8F%EF%BD%8E(javascript:alert(1))}

%3C/style%3E&search=Accept-Encoding:%20gzip,%20deflate%20Accept-Language:%20tr-TR,tr;q=0.9,en-US;q=0.8,en;q=0.7%20Cookie:%20PHPSESSID=u1j76fmkbd0010si77f5aig0ol
Accept-Encoding: gzip, deflate
Cookie: PHPSESSID=noouho4n0rocd92g43hgb6oq6h
--
HTTP/1.1 200 OK
Last-Modified: Wed, 17 Dec 2014 15:49:52 GMT
ETag: "16dc5-50a6b6d1dc800-gzip"
Accept-Ranges: bytes
Vary: Accept-Encoding
Content-Encoding: gzip
Content-Length: 33433
Keep-Alive: timeout=5, max=100
Connection: Keep-Alive
Content-Type: application/javascript

ADDITIONAL:

jquery-1.8.3.min.js from Adobe (musecdn.businesscatalyst.com) server
[here|https://community.adobe.com/t5/muse-discussions/missing-jquery-1-8-3-min-js-from-adobe-musecdn-businesscatalyst-com-server/td-p/11908671
]
there will be no phone or chat support for Adobe Muse. This forum will remain open for user to user interactions but will have no employee presence or support.
For those of you that are still subscribed, attacker can continue using Muse and will be able to open and edit existing websites or create new websites with the application.
So Attacker use this apportunity to send js file on target

Jqu ery : jquery is a package that makes things like HTML document traversal and manipulation, event handling, animation, and Ajax much simpler with an easy-to-use API that works across a multitude of browsers.

[here|https://security.snyk.io/package/npm/jquery/1.8.3
]

Use Cookie: PHPSESSID=u1j76fmkbd0010si77f5aig0ol to target of malicious server 24 times. just for this host.
The MITRE CVE dictionary describes this issue as:
jQuery before 3.0.0 is vulnerable to Cross-site Scripting (XSS) attacks when a cross-domain Ajax request is performed without the dataType option, causing text/javascript responses to be executed.

CVE-2015-9251
CVSS Version 3.x Base Score: 6.1 Medium ON NVD

RECOMAND: Regularly check for updates, conduct security assessments, and stay informed about the latest threats.

Verify the Vulnerability: Ensure that your website is indeed vulnerable to CVE-2015-9251. You can do this by checking the version of the software or component in question and comparing it to the information provided in the CVE report.

Apply Patches or Updates: If there is a patch or update available to fix the vulnerability, apply it as soon as possible. This is often the most straightforward and effective way to address the issue.

Review Configuration: Review the configuration settings of the software to make sure it is properly configured. Sometimes vulnerabilities can be exploited due to misconfigurations.

Security Audits: Conduct a security audit of your website to identify any potential vulnerabilities. Automated tools and manual testing can be used for this purpose.

And WAF gonna helpful too.