



# PHILIPS

## Security Testing Report

EDI\Interoperability Solutions

XDS 2023-1

PHILIPS SCOE



Confidential

This document is proprietary and confidential. No part of this document may be disclosed in any manner to a third party without the prior written consent of Philips Product Security and Services Office (PSSO).



Printed copies are uncontrolled unless authenticated.



## Table of Contents

Document Version Control.....	3
Document History .....	3
Distribution List .....	5
1. Definitions & Abbreviations .....	6
2. System Details & Architecture.....	7
3. Scope .....	9
4. Out of Scope.....	10
5. Executive Summary .....	11
6. Vulnerability Summary .....	13
7. Observations.....	14
8. Detailed Vulnerability Report.....	18
8.1 Webapp: Using Known Vulnerable Components .....	18
8.2 Webapp: Broken Access Control .....	23
8.3 Webapp: Weak Password Policy .....	28
8.4 Webapp: DOM Cross-Site Scripting (XSS).....	32
8.5 Webapp: Weak Input Validation .....	36
8.6 Webapp: Improper Error & Exception Handling .....	39
8.7 Webapp: Sensitive Information in the URL .....	42
8.8 Webapp: HTTP Strict Transport Security (HSTS) Not Implemented.....	45
8.9 Webapp: No Account Lockout Policy .....	48
8.10 Webapp: Reflected Cross-Site Scripting (XSS).....	51
8.11 Webapp: Weak SSL/TLS Configuration.....	57
9. Tools Used .....	59
10. Automated Tool Report.....	59
11. Manual Test Reports and Test Case Execution .....	60

PHILIPS SCOE



Confidential

This document is proprietary and confidential. No part of this document may be disclosed in any manner to a third party without the prior written consent of Philips Product Security and Services Office (PSSO).



Printed copies are uncontrolled unless authenticated.



## Document Version Control

<b>Name of the document : XDS 2023-1 Security Testing Report</b>		
<b>Version:</b> 7.0	<b>Intake ID:</b>	2648
<b>Document Definition:</b> This document highlights the vulnerabilities currently existing in the application under scope. It also documents possible actions to be taken to reduce/eliminate the vulnerabilities.	<b>Document ID:</b>	PRHC/C40/SVN/86070
<b>Author:</b> Raj Kiran Rudrapati	<b>Effective Date:</b>	09/Jun/2023
<b>Reviewed by:</b> Aravind C Ajayan		

## Document History

Version	Date	Author	Section	Changes
0.1	20/Jul/2020	Narendra Makkenna	Complete	Initial Draft
1.0	20/Jul/2020	Taksh Medhavi	Complete	Addition & review
1.1	01/Mar/2021	Shabana Bagum	Complete	Initial Draft
1.2	02/Mar/2021	K K Ashwin	Complete	Addition & review
2.0	03/Mar/2021	Narendra Makkenna	Complete	Final review
2.1	03/March/2022	Shibija K	Complete	Initial Draft
2.2	04/March/2022	K K Ashwin	Complete	Addition & review

PHILIPS SCOE



Confidential

This document is proprietary and confidential. No part of this document may be disclosed in any manner to a third party without the prior written consent of Philips Product Security and Services Office (PSSO).



Printed copies are uncontrolled unless authenticated.



3.0	04/March/2022	Pranati Mohanty	Complete	Final review
3.1	27/May/2022	Sreerag M	Vuln 8.2,8.4,8.6 and 8.11	Retest
3.2	27/May/2022	Shibija K	Vuln 8.2,8.4,8.6 and 8.11	Addition & review
4.0	27/May/2022	Pranati Mohanty	Vuln 8.2,8.4,8.6 and 8.11	Final Review
4.1	27/Aug/2022	Kartik Lalan	Complete	Addition & review
5.0	29/Aug/2022	Shibija K	Complete	Final Review
5.1	31/Jan/2023	Ashwin K K	Vuln 8.2,8.4,8.6 and 8.11	New feaure and retest
5.2	01/Feb/2023	Shibija K	Complete	Addition & technical review
6.0	01/ Feb /2023	Pranati Mohanty	Complete	Final Review
6.1	08/Jun/2023	Raj Kiran Rudrapati	Complete	Issue revalidation & Rapid test
7.0	09/Jun/2023	Aravind C Ajayan	Complete	Addition & Review

PHILIPS SCOE



Confidential

This document is proprietary and confidential. No part of this document may be disclosed in any manner to a third party without the prior written consent of Philips Product Security and Services Office (PSSO).



Printed copies are uncontrolled unless authenticated.



## Distribution List

User/Department/Stakeholder	E-Mail ID
Project Owner and PSO	<a href="mailto:subhash.naga@philips.com">subhash.naga@philips.com</a> ; <a href="mailto:Stephanie.Heidstra@philips.com">Stephanie.Heidstra@philips.com</a> ; <a href="mailto:moin.creemers@philips.com">moin.creemers@philips.com</a> ; <a href="mailto:ManishKumar.MachingalSukumar@philips.com">ManishKumar.MachingalSukumar@philips.com</a> ; <a href="mailto:Stephanie.Heidstra@philips.com">Stephanie.Heidstra@philips.com</a> ; <a href="mailto:chidamber.kumar_1@philips.com">chidamber.kumar_1@philips.com</a> ; <a href="mailto:abhishek.kumar.pathak@philips.com">abhishek.kumar.pathak@philips.com</a> ; <a href="mailto:revathi.r@philips.com">revathi.r@philips.com</a>

PHILIPS SCOE



Confidential

This document is proprietary and confidential. No part of this document may be disclosed in any manner to a third party without the prior written consent of Philips Product Security and Services Office (PSSO).



Printed copies are uncontrolled unless authenticated.



## 1. Definitions & Abbreviations

Term	Explanation
SCoE	Security Center of Excellence
TLS	Transport Layer Security
SSL	Secure Socket Layer
XSS	Cross Site Scripting

The severity of every vulnerability has been calculated by using industry standard **Common Vulnerability Scoring System (CVSS)** used for assessing the severity of computer system vulnerabilities. CVSS provides a way to capture the principal characteristics of a vulnerability and produce a numerical score (Scores range from 0 to 10, with 10 being the most severe) reflecting its severity. The numerical score can then be translated into a qualitative representation (such as low, medium, high, and critical) to help organization properly assess and prioritize their vulnerability management processes.

The severity rating for the numerical values are mapped below:

None	0.0
Low	0.1 - 3.9
Medium	4.0 - 6.9
High	7.0 - 8.9
Critical	9.0 - 10.0

The **Severity** and **CVSS vector** of each vulnerability is calculated using the CVSS V3 **Base Score Metrics** Calculator located [here](#). Vulnerabilities identified during security assessment are classified into standardized categories. Refer following table for more information:

Categories for vulnerability classification

Web application security assessment	OWASP Top Ten - 2021
Mobile application security assessment	OWASP Top Ten - 2016
IoT/Hardware security assessment	OWASP Top Ten – 2014

PHILIPS SCOE



Confidential

This document is proprietary and confidential. No part of this document may be disclosed in any manner to a third party without the prior written consent of Philips Product Security and Services Office (PSSO).



Printed copies are uncontrolled unless authenticated.



## 2. System Details & Architecture

Brief about the product architecture:

Philips Interoperability Solutions (formerly Forcare) is an open-standard-based interoperability software solutions for fast and flawless data flows between medical systems and information sources at the departmental and enterprise levels, as well as Health Information Exchanges (HIEs) across health systems.

The tested components: ForView, ForAudit ForImageUpload and ForAdmin web application.

**ForAdmin** - ForAdmin is a web-based application for system administrators. This can be used for configuring and monitoring the Forcare application components in your network. With ForAdmin, you can make configuration changes at runtime without requiring restarting your server. Component configurations are stored in XML files that are validated to prevent basic configuration errors.

**ForView**- ForView is an application for care providers that lets them find, view, and share patient-oriented clinical information. ForView complements existing clinical information systems, adding the ability to view documents and images from a variety of sources that are not limited to one specific institution or document type.

**ForAudit**- ForAudit is an IHE ATNA Audit Repository. It captures audit logs sent via UDP or TCP/SSL (syslog, per IHE ITI ATNA) and supports HTTP or HTTPS based audit transactions.

**ForImageUpload**- ForImageUpload is an application to upload Dicom/Zip files of images.

PHILIPS SCOE

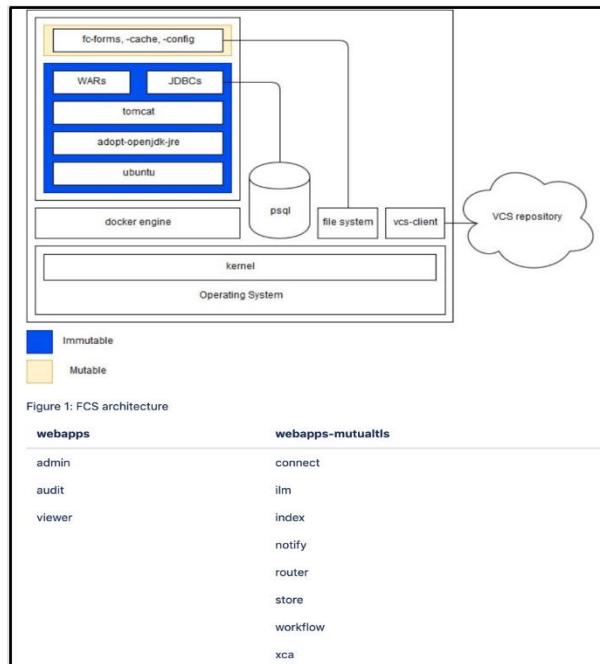


Confidential

This document is proprietary and confidential. No part of this document may be disclosed in any manner to a third party without the prior written consent of Philips Product Security and Services Office (PSSO).



Printed copies are uncontrolled unless authenticated.



The environment provided for security testing is a Pentest Environment.

PHILIPS SCOE



Confidential

This document is proprietary and confidential. No part of this document may be disclosed in any manner to a third party without the prior written consent of Philips Product Security and Services Office (PSSO).



Printed copies are uncontrolled unless authenticated.



### 3. Scope

The scope of this security assessment is to perform **Grey box** security testing to find security threats that may come from a malicious outsider or insider user of the **XDS 2023-1**. Security testing on **Web applications (Viewer,Audit,Admin&ImageUpload)** of **XDS 2023-1** is performed.

The following list includes some examples of major activities performed during the assessment:

#### Web Application:

- Crawl through complete scope of the web application/service space and identify for any unauthenticated URL or directory.
- Check for all input injection-based attacks across all the possible entry fields in Web API.
- Exploiting any known component vulnerability or service misconfiguration.
- Reviewing the transport layer security implemented.

*Follow “[Test case execution](#)” section to get the detailed about test*

Type	Scope of Assessment		
Web Application	XDS	URL	<a href="https://server_url/admin">https://server_url/admin</a> <a href="https://server_url/audit">https://server_url/audit</a> <a href="https://server_url/imageupload">https://server_url/imageupload</a> <a href="https://server_url/viewer">https://server_url/viewer</a>
		Version	2023-1
		Environment	Pentest
		User Roles	root (self creatable user roles)

\* server\_url – During the assessment, the server IP was changed couple of times. The IP's are listed below. So in this document, url is referred to as ‘server\_url’.

IP's:

<https://3.67.186.182/>

<https://18.196.27.233/>

<https://3.71.200.223/>

PHILIPS SCOE



Confidential

This document is proprietary and confidential. No part of this document may be disclosed in any manner to a third party without the prior written consent of Philips Product Security and Services Office (PSSO).



Printed copies are uncontrolled unless authenticated.



**Note (09/06/2023):** The scope of the testing is to evaluate 2 new features deployed as part 2022-4 release and revalidate previous open vulnerabilities and a rapid testing of the application functionalities in limited time frame & below changes:

- The scope of the testing is to validate the application functionalities related to the issues (DEF-6166, DEF-6242, DEF-6284, DEF-6709, DEF-6813, DEF-6816, DEF-6831) and a rapid testing of the application functionalities.
- Scope of the testing is to make sure that the fixes do not introduce any security vulnerabilities.

## 4. Out of Scope

Below mentioned items are out of scope for the current security assessment:

- Source code review
- Cloud Testing
- Docker Testing
- Complete security assessment of 4 portals

**Note:** We have covered the testing of **XDS 2023-1** in the environment provided and the results are valid if the same environment is replicated. Re-run the tests if a new propagation of the environment is made.

PHILIPS SCOE



Confidential

This document is proprietary and confidential. No part of this document may be disclosed in any manner to a third party without the prior written consent of Philips Product Security and Services Office (PSSO).



Printed copies are uncontrolled unless authenticated.



## 5. Executive Summary

Security Center of Excellence (SCoE) team is engaged in activities to conduct security assessment of **XDS 2023-1** which included **Web applications** in scope. The purpose of the engagement is to evaluate the security of the **XDS 2023-1** against industry best practice criteria.

Note: Only highlights of important vulnerabilities are described below. Please refer 'Vulnerability Summary' section for complete detailed list of vulnerabilities.

During the security assessment following factors are found with consideration for significant improvement:

- Using known vulnerable components
- Weak input validations
- Likelihood of cross site scripting
- Weak cipher suite used
- Multiple security misconfigurations
- Weak password policy on Foradmin portal

During the security assessment of the product, security issues in the below areas are not found:

- Cross site request forgery
- Token Management

PHILIPS SCOE



Confidential

This document is proprietary and confidential. No part of this document may be disclosed in any manner to a third party without the prior written consent of Philips Product Security and Services Office (PSSO).

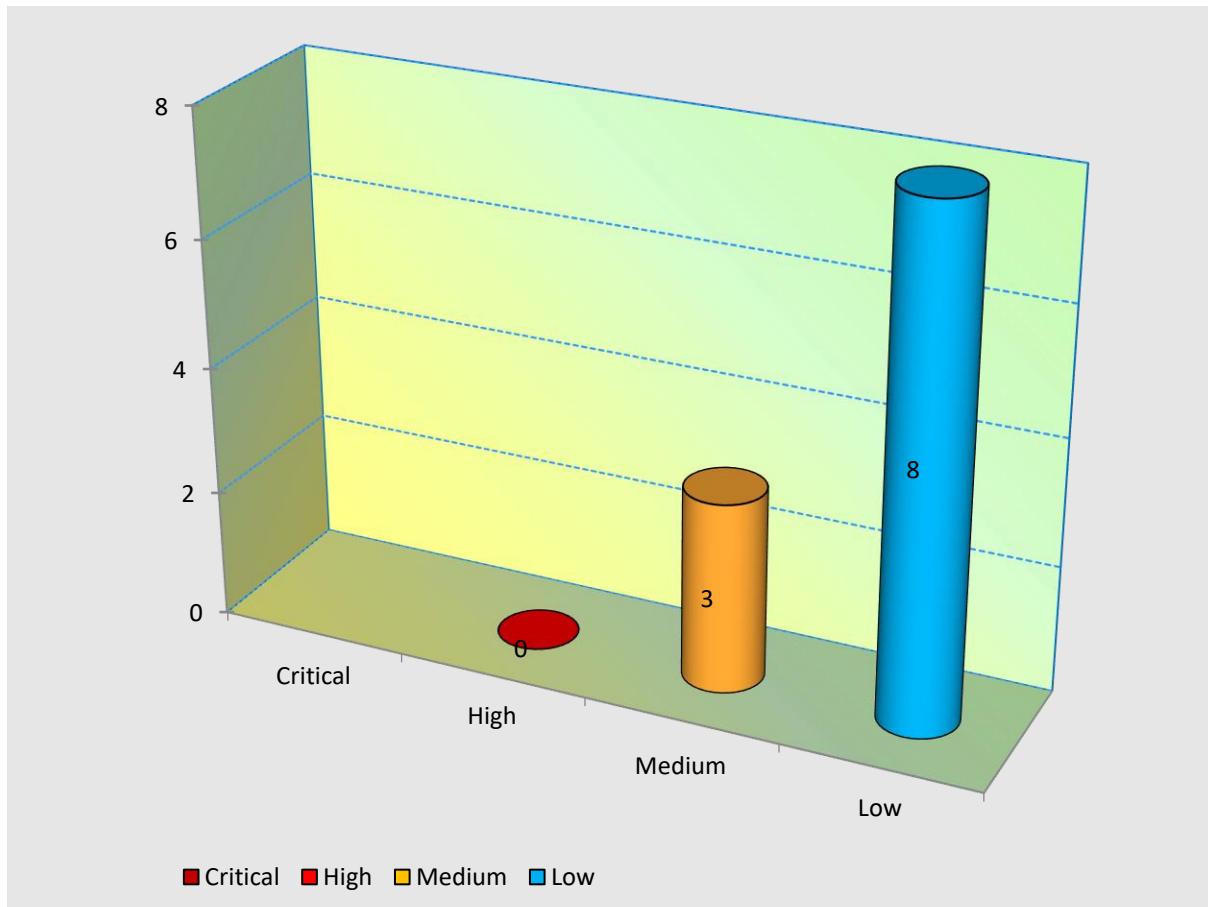
11

Printed copies are uncontrolled unless authenticated.

## VULNERABILITY SUMMARY CHART

The graph below shows a summary of the number of vulnerabilities and their severities.

**Note:** The vulnerabilities mentioned in this report are technical vulnerabilities only. The Product Security Risk Assessment would report the business risks associated with these vulnerabilities.



PHILIPS SCOE



Confidential

This document is proprietary and confidential. No part of this document may be disclosed in any manner to a third party without the prior written consent of Philips Product Security and Services Office (PSSO).



Printed copies are uncontrolled unless authenticated.



## 6. Vulnerability Summary

The findings and vulnerabilities from the assessment are explained in the below table:

Finding No.	Vulnerability Title	Technical Risk	Impacted Area	CVE ID*	Status	Status(31st Jan 23)	Status(6th Jun 23)
30132	Using Known vulnerable components	Medium	Webapp	Refer 8.1	Open	Open	Open
79143	Broken Access Control	Medium	Webapp	NA	Open	Open	Open
30136	Weak Password Policy	Medium	Webapp	NA	Open	Open	Open
77505	DOM Cross Site Scripting	Low	Webapp	NA	Open	Open	Open
30145	Weak Input Validation	Low	Webapp	NA	Open	Open	Open
30209	Improper error & exception handling	Low	Webapp	NA	Open	Open	Open
37688	Sensitive information in the URL	Low	Webapp	NA	Open	Open	Open
30128	HTTP Strict Transport Security (HSTS) Not Implemented	Low	Webapp	NA	Open	Open	Open
30146	No Account Lockout Policy	Low	Webapp	NA	Open	Open	Open
30125	Reflected Cross-Site Scripting (XSS)	Low	Webapp	NA	Open	Open	Open
83850	Weak SSL/TLS Configuration	Low	Webapp	NA	-	New	Open

\*CVE ID are mentioned for the vulnerabilities which has a known external CVE.

PHILIPS SCOE



Confidential

This document is proprietary and confidential. No part of this document may be disclosed in any manner to a third party without the prior written consent of Philips Product Security and Services Office (PSSO).



Printed copies are uncontrolled unless authenticated.



## 7. Observations

Below mentioned observations are not considered as vulnerability but informative to the business.

*Observations which shows good implementation or best practice identified:*

- XSS protection flag is enabled.

```
Target: https://3.71.200.223

Send Cancel < > +
```

Request

Pretty	Raw	Hex
1 GET /viewer/services/all/list.json?patientID=35e6924500&patientIDAuth=1.3.6.1.4.1.21367.2005.3.7		
2 Host: 3.71.200.223		
3 Cookie: JSESSIONID=SCDADFL1Z7A01277F7B24D0F7E89E9AE		
4 See-Header: "Noti-A-Brand":v="88", "Chromium":v="112"		
5 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win32) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/112.0.5613.100 Safari/537.36		
6 Accept: */*		
7 Sec-Fetch-Site: none-origin		
8 Sec-Fetch-Mode: empty		
9 Referer: https://3.71.200.223/viewer/patient/query.html		
10 Accept-Encoding: gzip, deflate		
11 Accept-Language: en-US,en;q=0.9		
12		

Response

Pretty	Raw	Hex	Render
1 HTTP/2 200 OK			
2 Cache-Control: no-store, no-cache, must-revalidate			
3 Pragma: no-cache			
4 Content-Type: application/json;charset=UTF-8			
5 Date: Mon, 05 Jun 2023 09:13:52 GMT			
6 Content-Length: 12546			
7 Forwarded-For-LogonText: 79d8f001e495/viwer-287			
8 Vary: accept-encoding			
9 X-Content-Type-Options: nosniff			
10 X-Xss-Protection: 1; mode=block			
11 Content-Type: application/pdf			
12			
13 {			
14 "result":{			
15 "warnings":{			
16 "documents":{			
17 "mimeType": "application/pdf",			
18 "id": "#fc3770-eec-bcbe-bead-74e137d9f59",			
19 "logicalId": "fc3770-eec-bcbe-bead-74e137d9f59",			
20 "name": "STABLE DOCUMENT",			
21 "version": "1.3",			
22 "creationTime": "19860331T000000Z",			
23 "hash": "a1C274500B18c027A5eBcd17a16b3d57b526",			
24 "languageCode": "en-US",			
25 "repositoryType": "1.2.3",			
26 "serviceStopTime": "19860331T000000Z",			
27 "serviceStopTime": "19860331T000000Z",			
28 "size": "64KB",			
29 "source": "https://35e6924500***41.3.6.1.4.1.21367.2005.3.74180",			
30 "sourcePatientInfo":{			
31 "PID-11":5624800***41.3.6.1.4.1.21367.2005.3.74180*,			
32 "PID-11":5624800***41.3.6.1.4.1.21367.2005.3.74180*,			
33 "PID-11":5624800***41.3.6.1.4.1.21367.2005.3.74180*,			
34 "PID-11":5624800***41.3.6.1.4.1.21367.2005.3.74180*,			
35 "PID-11":5624800***41.3.6.1.4.1.21367.2005.3.74180*,			
36 "documentAvailability": "Online",			
37 }			

- Image Upload feature has proper restriction in place for rejecting unintended malicious files as part ZIP and DICOMDIR functionality.

ad M

<https://ec2-3-70-166-239.eu-central-1.compute.amazonaws.com/imageupload/?assigningAuthority=1.3.6.1.4.1.21367.2005.3.7#>

 SELECT     EDIT     SEND

Patient demographics

Patient ID:	134442134
Given Name:	
Last Name:	Gerrit Getal
Date of Birth:	Feb 15, 1978 

Select one or more studies.

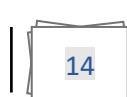
June 1, 2011, CT, Studies - Series - Instances, Accession#: 11212

The following files cannot be uploaded:  
</pentest/Launch.ica>

- File upload accepts EICAR virus characters but the server quarantines this particular portion of file. When we download this upload again, one file where we injected the payload is not present in the ZIP file.

PHILIPS SCUE

Confidential



This document is proprietary and confidential. No part of this document may be disclosed in any manner to a third party without the prior written consent of Philips Product Security and Services Office (PSSO).

Printed copies are uncontrolled unless authenticated.



The screenshot shows the Network tab in the Chrome DevTools. It displays two entries: a 'Request' and a 'Response'. The 'Request' entry shows a POST method with various headers like Accept-Encoding, Accept-Language, and Content-Disposition. The 'Content-Disposition' header specifies the file name as 'IMG00000.dcm'. The 'Response' entry shows a successful HTTP 200 OK status with various headers including Cache-Control, Content-Type, and Expires. The response body contains JSON data with a 'status' field set to 'success'. The 'Inspector' panel on the right is visible, showing tabs for Request Attributes, Request Query Parameters, Request Body Parameters, Request Cookies, Request Headers, and Response Headers.

Request	Response	Inspector
Pretty Raw Hex	Pretty Raw Hex Render	Request Attributes
17 Accept-Encoding: gzip, deflate 18 Accept-Language: en-US,en;q=0.9 19 20 -----WebKitFormBoundarysdSy3YOACBqvPBN 21 Content-Disposition: form-data; name="patient.id" 22 23 13444C134***41.3.6.1.4.1.21367.2005.3.74ISO 24 -----WebKitFormBoundarysdSy3YOACBqvPBN 25 Content-Disposition: form-data; name="document.content"; filename="IMG00000.dcm" 26 Content-Type: application/octet-stream 27 28 GE Medical Systems/DICOM Part 10 fileIDMULACBU11.2.840.10008.5.1.4.1.1.7UI61.2.826.0.1.3 60043.2.1208.35045845353201152611242924U1.2.840.10008 .1.2.1UI1.2.528.1.1001.2.20040707.SHANIM DICOM03.2 CS 29 ISO_14159_P48AP[4\PKZx4(P")7CC7]\$EICAR-STANDARD-ANTIVIR US-TEST-FILE\$H+H# 100CS0RIG1NLY(PRIMARY OTHERDA20110601T112429.000000011. 2.840.10008.5.1.4.1.1.7UI61.2.826.0.1.3680043.2.1208.350 48545353201152611242924	1 HTTP/2 200 OK 2 Cache-Control: no-store, no-cache, must-revalidate 3 Cache-Control: post-check=0, pre-check=0 4 Content-Type: application/json 5 Date: Tue, 24 Jan 2023 09:23:54 GMT 6 Expires: 0 7 Forcare.com-LogContext: adf9e6be2eb/connect-984 8 X-Content-Type-Options: nosniff 9 X-Frame-Options: SAMEORIGIN 10 X-Xss-Protection: 1; mode=block 11 Content-Length: 23 12 13 { 14   "status": "success" 15 }	Request Query Parameters Request Body Parameters Request Cookies Request Headers Response Headers

*Observations which shows missing best practice or possible weak implementation (this may/may not be direct active threat):*

- No email verification while registering the user.
  - Password is created by admin user, No password change option available at other applications.
  - Application is allowing simultaneous session logons.
  - Even though, there are 2 sets of authentication parameters (JSESSIONID & Authorization Token), some of the functionalities of the application is accessible with just either one of the parameters.
  - Also, we highly recommend enforcing jwt token for authentication/authorization rather than relying up on either of the above-mentioned authentication mechanisms.
  - Password is in plain text at admin portal in the configurations.

PHILIPS SCOE

Confidential

This document is proprietary and confidential. No part of this document may be disclosed in any manner to a third party without the prior written consent of Philips Product Security and Services Office (PSSO).



- ImageUpload Online help page does not require any authentication. Since there is no PII or PHI we are marking this as Observation.

Send Cancel < > **Target: https://ec2-3-70-166-239.eu-central-1.compute.amazonaws.com**

Request	Response	Inspector
<pre>Pretty Raw Hex 1 GET /imageupload/2004-6/forcare/imageupload/help/en/help.htm 1 HTTP/2 2 Host: ec2-3-70-166-239.eu-central-1.compute.amazonaws.com 3 Content-Length: 2 4 5 6</pre>	<pre>Pretty Raw Hex Render ImageUpload - Online help</pre> <h2>General</h2> <p>The Forcare Image Upload can be used to manually upload medical images in DICOM format to be shared with one or more other physicians. There are two ways to upload DICOM images: using a DICOMDIR file with corresponding DICOM files or using a ZIP file containing the DICOM files. Please note that depending on the configuration of your system any of these two options may not be available.</p> <h3>Browser support</h3> <p>Uploading using a DICOMDIR and a ZIP file is supported by:</p> <ol style="list-style-type: none"><li>1. Microsoft Edge</li><li>2. Google Chrome</li><li>3. Mozilla Firefox</li></ol> <p>Internet Explorer 11 and Safari browsers only support uploading using a ZIP file.</p>	<p>Request Attributes Request Query Parameters Request Body Parameters Request Cookies Request Headers Response Headers</p>

RabbitMQ

- Default credentials found in environment variable for rabbitmq

- The bind mounts has Read Write enabled which is not a good implementation from security standpoint.

PHILIPS SCOE

Confidential

This document is proprietary and confidential. No part of this document may be disclosed in any manner to a third party without the prior written consent of Philips Product Security and Services Office (PSSO).



```

ubuntu@ip-10-0-1-71: ~
{
  "State": {
    "Status": "running",
    "Running": true,
    "Paused": false,
    "Restarting": false,
    "OOMKilled": false,
    "Dead": false,
    "Pid": 2007,
    "ExitCode": 0,
    "Error": "",
    "StartedAt": "2023-01-18T10:19:02.752113849Z",
    "FinishedAt": "2023-01-18T14:34:41.312508459Z"
  },
  "Image": "sha256:6975b45ffcc3102d20d7e0bde94d2180b76c73c22847161000f439b10e0f7c2",
  "ResolveConfPath": "/var/lib/docker/containers/35702e104bd73d93d664abe38f404776278ef5d1d79c0fa2a15f04c9c0a9955e/resolv.conf",
  "HostnamePath": "/var/lib/docker/containers/35702e104bd73d93d664abe38f404776278ef5d1d79c0fa2a15f04c9c0a9955e/hostname",
  "HostsPath": "/var/lib/docker/containers/35702e104bd73d93d664abe38f404776278ef5d1d79c0fa2a15f04c9c0a9955e/hosts",
  "LogPath": "/var/lib/docker/containers/35702e104bd73d93d664abe38f404776278ef5d1d79c0fa2a15f04c9c0a9955e/35702e104bd73d93d664abe38f404776278ef5d1d79c0fa2a15f04c9c0a9955e-json.log",
  "Name": "fc-all-in-one_rabbitmq_1",
  "RestartCount": 0,
  "Driver": "overlay2",
  "Platform": "linux",
  "MountLabel": "",
  "ProcessLabel": "",
  "AppArmorProfile": "docker-default",
  "ExecDriver": "native",
  "HostConfig": {
    "Binds": [
      "/home/forcare/fc-all-in-one/rabbitmq/config:/etc/rabbitmq/conf.d:rw",
      "/home/forcare/fc-all-in-one/rabbitmq/certificates:/etc/rabbitmq/certificates:rw",
      "/home/forcare/fc-all-in-one/rabbitmq/logs:/etc/rabbitmq/logs:rw"
    ],
    "ContainerIDFile": ""
  }
}

```

```

    "Name": "overlay2"
  },
  "Mounts": [
    {
      "Type": "bind",
      "Source": "/home/forcare/fc-all-in-one/rabbitmq/certificates",
      "Destination": "/etc/rabbitmq/certificates",
      "Mode": "rwm",
      "RW": true,
      "Propagation": "rprivate"
    },
    {
      "Type": "bind",
      "Source": "/home/forcare/fc-all-in-one/rabbitmq/config",
      "Destination": "/etc/rabbitmq/conf.d",
      "Mode": "rwm",
      "RW": true,
      "Propagation": "rprivate"
    },
    {
      "Type": "bind",
      "Source": "/home/forcare/fc-all-in-one/rabbitmq/logs",
      "Destination": "/etc/rabbitmq/logs",
      "Mode": "rwm",
      "RW": true,
      "Propagation": "rprivate"
    },
    {
      "Type": "volume",
      "Name": "8a10c263f350824d5ae83fd4eba6bc5f885b2199905ea70d4f6d07289f204c4",
      "Source": "/var/lib/docker/volumes/8a10c263f350824d5ae83fd4eba6bc5f885b2199905ea70d4f6d07289f204c4/_data",
      "Destination": "/var/lib/rabbitmq",
      "Driver": "local",
      "Mode": "",
      "RW": true,
      "Propagation": ""
    }
  ]
}

```



## 8. Detailed Vulnerability Report

### 8.1 Webapp: Using Known Vulnerable Components

Vulnerability Title	Using Known Vulnerable Components
Vulnerability Category	A6 Vulnerable and Outdated Components
Severity	Medium
CVSS V3 Calculation	CVSS Base Score: 4.8 CVSS:3.0/ AV:N/AC:H/PR:N/UI:N/S:U/C:L/I:L/A:N
Description	<p><b>Vulnerability Description:</b> During the security assessment of the product, it is observed that the web application is using components with known vulnerabilities and associated CVEs.</p> <p>Technologies are like jquery-1.2.6, dojo 1.9.6 and AngularJS v1.8.2 have known CVE IDs:</p> <p>jquery-1.2.6, AngularJS v1.8.2, and dojo 1.9.6</p> <ul style="list-style-type: none"> <li>• moment.js 2.29.3 - <a href="#">CVE-2022-31129</a></li> <li>• jquery-1.2.6 - <a href="https://nvd.nist.gov/vuln/detail/CVE-2011-4969">https://nvd.nist.gov/vuln/detail/CVE-2011-4969</a></li> <li>• AngularJS v1.8.2 - <a href="#">angular 1.8.2 vulnerabilities   Snyk</a></li> <li>• Dojo 1.9.6 - <a href="https://security.snyk.io/package/npm/dojo/1.9.2">https://security.snyk.io/package/npm/dojo/1.9.2</a></li> </ul> <p>AngularJS LTS discontinued.</p> <p><a href="#">Discontinued Long Term Support for AngularJS   by Mark Thompson (@marktechson)   Angular Blog</a></p> <p><b>Retest (02-Jun-2023):</b> It is observed that the server makes use of the mentioned vulnerable component. jquery-1.2.6, AngularJS v1.8.2, moment.js 2.29.3 and dojo 1.9.6 are being used. jQuery 1.x and 2.x are End-of-Life and no longer receiving security updates</p> <p><b>Retest (30-Jan-2023):</b> It is identified that the server makes use of AngularJS which has reached end of life. Server banner disclosure is also happening as part of server response. It is observed Apache Tomcat/9.0.68 is been used by the application.</p>

PHILIPS SCOE



Confidential

This document is proprietary and confidential. No part of this document may be disclosed in any manner to a third party without the prior written consent of Philips Product Security and Services Office (PSSO).



Printed copies are uncontrolled unless authenticated.



	<p><b>Exploitability Rational:</b> Published vulnerabilities have a greater likelihood of exploitation by attackers due to readily available proof-of-concept code that exploits the issue, or integrates the exploits into freely available testing tools.</p> <p><b>Impact Rational:</b> Depending on the nature of known vulnerabilities, this can allow an attacker to compromise the server and any data stored within.</p>
Affected Systems/IP Address/URL	<p><b>Retest (02-Jun-2023):</b></p> <p><a href="https://server_url/admin/">https://server_url/admin/</a></p> <p><a href="https://server_url/viewer/">https://server_url/viewer/</a></p> <p><a href="https://server_url/audit/">https://server_url/audit/</a></p> <p><b>Old POC:</b></p> <p><a href="https://ec2-3-70-166-239.eu-central-1.compute.amazonaws.com/admin">https://ec2-3-70-166-239.eu-central-1.compute.amazonaws.com/admin</a></p> <p><a href="https://ec2-3-70-166-239.eu-central-1.compute.amazonaws.com/viewer">https://ec2-3-70-166-239.eu-central-1.compute.amazonaws.com/viewer</a></p> <p><a href="https://ec2-3-70-166-239.eu-central-1.compute.amazonaws.com/viewer/2204-47/js/angular/angular.min.js">https://ec2-3-70-166-239.eu-central-1.compute.amazonaws.com/viewer/2204-47/js/angular/angular.min.js</a></p>
Recommendation	Service version is vulnerable to an attack, take preventative measures to mitigate the vulnerability until an upgrade or patch is released.
Status	<b>Open</b>

### Steps to Reproduce

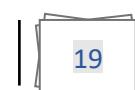
Steps same as before

PHILIPS SCOE



Confidential

This document is proprietary and confidential. No part of this document may be disclosed in any manner to a third party without the prior written consent of Philips Product Security and Services Office (PSSO).



Printed copies are uncontrolled unless authenticated.



Not secure | https://18.196.27.233/admin/login.html

**Retire.js**

dojo 1.9.6 Found in https://18.196.27.233/admin/2301-26/js/dojo/dojo.js \_\_\_\_\_ Vulnerability info:

Medium	307
High	CVE-2018-15494
High	CVE-2020-5258 GHSA-jxfh-8wgv-vf72
High	Prototype pollution CVE-2021-23450 GHSA-m8gw-hjpr-rj7

Enabled Show unknown [1] [2] [3] [4] [5] [6] Save

**FORADMIN**

User Name  Password

Login

DEVELOPMENT SOFTWARE - Not for clinical use  
Version: 2021-1

FORCARE

O  
audit\_login\_pg\_onl  
y.html

O  
viewer\_retirejs.html

Not secure | https://3.71.200.223/viewer/patient/

**HTTP Status 404 – Not Found**

Type Status Report

Message The requested resource [/viewer/patient/] is not available

Description The origin server did not find a current representation for the target resource or is not willing to disclose that one exists.

Apache Tomcat/9.0.71

Old POC:

- Launch the application and run retire.js plugin.
- Login to any application ForAdmin, ForView.

ForView Portal

PHILIPS SCOE



Confidential

This document is proprietary and confidential. No part of this document may be disclosed in any manner to a third party without the prior written consent of Philips Product Security and Services Office (PSSO).



Printed copies are uncontrolled unless authenticated.



Not secure | <https://ec2-3-70-166-239.eu-central-1.compute.amazonaws.com/viewer/patient/query.html>

Enabled

### Retire.js

angularjs	1.8.2	Found in https://ec2-3-70-166-239.eu-central-1.compute.amazonaws.com/viewer/2204-47/js/angular/angular.min.js Vulnerability info: Low End-of-Life: Long term support for AngularJS has been discontinued 54	[1]
angularjs	1.8.2	Found in https://ec2-3-70-166-239.eu-central-1.compute.amazonaws.com/viewer/2204-47/js/angular/angular.min.js Vulnerability info: Low End-of-Life: Long term support for AngularJS has been discontinued 54	[1]
dojo	1.9.6	Found in https://ec2-3-70-166-239.eu-central-1.compute.amazonaws.com/viewer/2204-47/js/dojo/dojo.js Vulnerability info: Medium 307 [1] [2] High CVE-2018-15494 [1] Medium CVE-2020-5258 [1] Medium Prototype pollution CVE-2021-23450 [1]	
jquery	1.2.6	Found in https://ec2-3-70-166-239.eu-central-1.compute.amazonaws.com/viewer/2204-47/js/simile-ajax/simile-ajax-bundle.js Vulnerability info: Medium CVE-2011-4969 XSS with location.hash [1] [2] Medium CVE-2012-6708 11290 Selector interpreted as HTML [1] [2] [3] Medium CVE-2019-11358 jQuery before 3.4.0, as used in Drupal, Backdrop CMS, and other products, mishandles jQuery.extend(true, {}, ...) because of Object.prototype pollution [1] [2] Medium CVE-2020-11022 Regex in its jQuery.htmlPrefilter sometimes may [1]	

## ForAdmin portal

Not secure | <https://ec2-3-70-166-239.eu-central-1.compute.amazonaws.com/admin/admin/overview.html>

Enabled

### Retire.js

dojo	1.9.6	Found in https://ec2-3-70-166-239.eu-central-1.compute.amazonaws.com/admin/2204-46/js/dojo/dojo.js Vulnerability info: Medium 307 [1] [2] High CVE-2018-15494 [1] Medium CVE-2020-5258 [1] Medium Prototype pollution CVE-2021-23450 [1]	
------	-------	---	--

Banner grabbing of Apache Tomcat server version.

PHILIPS SCOE



Confidential

This document is proprietary and confidential. No part of this document may be disclosed in any manner to a third party without the prior written consent of Philips Product Security and Services Office (PSSO).



Printed copies are uncontrolled unless authenticated.



← → ⌂ https://ec2-3-70-166-239.eu-central-1.compute.amazonaws.com/viewer/patient/

## HTTP Status 404 – Not Found

**Type** Status Report

**Message** The requested resource [/viewer/patient/] is not available

**Description** The origin server did not find a current representation for the target resource or is not willing to disclose that one exists.

**Apache Tomcat/9.0.68**

PHILIPS SCOE



Confidential

This document is proprietary and confidential. No part of this document may be disclosed in any manner to a third party without the prior written consent of Philips Product Security and Services Office (PSSO).



Printed copies are uncontrolled unless authenticated.



## 8.2 Webapp: Broken Access Control

Vulnerability Title	Broken Access Control
Vulnerability Category	A1 Broken Access Control
Severity	Medium
CVSS V3 Calculation	CVSS Base Score: 6.5 CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N
Description	<p><b>Vulnerability Description:</b></p> <p>The application allows lower privileged users to access resources or perform actions which is available to a higher level account. This usually occurs when the server does not perform authorization/entitlement checks on each request to ensure that the user has the appropriate privileges before executing the request, or when those checks are made based on values that can be tampered with on the client-side.</p> <p>It is observed that the user without SYSTEM_PHI_READ role defined can view/read the following API endpoints which consists of sensitive information like, backend components/versions, encryption password etc.</p> <p><b>Retest (02-Jun-2023):</b> It is observed that the issue is still persistent. During the assessment, it is observed that after some time, the token becomes unauthorized but still able to retrieve data.</p> <p><b>Retest (31-Jan-2023):</b> It is observed that user with SYSTEM_PHI_READ has view option on backend configuration which includes sensitive information. Issue still persists.</p> <p><b>Exploitability Rational:</b> The attacker can be any user who has access to the forcare admin application.</p> <p><b>Impact Rational:</b> Depending on the nature of the information, a malicious user may obtain personally identifiable information (PII), private user data or information which can allow user impersonation (in the event of credential or session identifier).</p>

PHILIPS SCOE



Confidential

This document is proprietary and confidential. No part of this document may be disclosed in any manner to a third party without the prior written consent of Philips Product Security and Services Office (PSSO).



Printed copies are uncontrolled unless authenticated.



	<p>Retest (02-Jun-2023):</p> <p><a href="https://server_url/admin/services/admin/components/viewer/status/retrieve.json?format=true">https://server_url/admin/services/admin/components/viewer/status/retrieve.json ?format=true</a></p> <p><a href="https://server_url/admin/services/admin/components/admin/config/properties.json">https://server_url/admin/services/admin/components/admin/config/properties.json</a></p> <p><a href="https://server_url/admin/services/admin/components/audit/editor/list.json">https://server_url/admin/services/admin/components/audit/editor/list.json</a></p> <p><a href="https://server_url/admin/services/admin/components/viewer/status/retrieve.json?format=true">https://server_url/admin/services/admin/components/viewer/status/retrieve.json ?format=true</a></p> <p><a href="https://server_url/admin/services/admin/components/admin/config/properties.json">https://server_url/admin/services/admin/components/admin/config/properties.json</a></p> <p><a href="https://server_url/admin/services/admin/queue/retrieve.json">https://server_url/admin/services/admin/queue/retrieve.json</a></p> <p><a href="https://server_url/admin/services/admin/components/audit/editor/list.json">https://server_url/admin/services/admin/components/audit/editor/list.json</a></p> <p><a href="https://server_url/viewer/2301-14/js/forcare/bo/PatientId.js">https://server_url/viewer/2301-14/js/forcare/bo/PatientId.js</a></p> <p>Old POC</p> <p><a href="https://ec2-3-70-166-239.eu-central-1.compute.amazonaws.com/admin/services/admin/components/viewer/status/retrieve.json?format=true">https://ec2-3-70-166-239.eu-central-1.compute.amazonaws.com/admin/services/admin/components/viewer/status/retrieve.json ?format=true</a></p> <p><a href="https://ec2-3-70-166-239.eu-central-1.compute.amazonaws.com/admin/services/admin/components/admin/config/properties.json">https://ec2-3-70-166-239.eu-central-1.compute.amazonaws.com/admin/services/admin/components/admin/config /properties.json</a></p> <p><a href="https://ec2-3-70-166-239.eu-central-1.compute.amazonaws.com/admin/services/admin/components/audit/editor/list.json">https://ec2-3-70-166-239.eu-central-1.compute.amazonaws.com/admin/services/admin/components/audit/editor /list.json</a></p> <p><b>Note: This is an application wide issue. Instances are not limited to the above items. Fix should be applied across the platform.</b></p>
<b>Recommendation</b>	Check and verify the privileges of the user and check or verify before serving the response.
<b>Status</b>	<b>Open</b>

PHILIPS SCOE



Confidential

This document is proprietary and confidential. No part of this document may be disclosed in any manner to a third party without the prior written consent of Philips Product Security and Services Office (PSSO).



Printed copies are uncontrolled unless authenticated.



## Steps to Reproduce

**Retest (02-Jun-2023):**

### **Case1:**

The steps same as before

### **Case2:**

Step1: Configure the browser with a proxy tool like Burp Suite and log into the foradmin application.

Step2: Leave the setup idle for about 5-10mins, the token becomes unauthorized.

Step3: Send the retrieve data request to repeater and observe the behavior.

## Supportive Evidence:

### **Case1:**

The screenshot shows two captured requests in Burp Suite's "Request" tab. Both requests are GETs to the URL `/admin/services/admin/components/connect/config/properties.json`. The first request has a status code of 200 and a response size of 5062 bytes. The second request also has a status code of 200 and a response size of 5062 bytes. The "Response" tab shows a large, redacted JSON object. The redaction covers several fields, including database configurations (PostgreSQL dialect, manager password, etc.), security settings (TLS 1.3, SNI), and various API keys and secrets. The "Inspector" tab on the right shows the request attributes, cookies, headers, and response headers.

PHILIPS SCOE

Confidential

This document is proprietary and confidential. No part of this document may be disclosed in any manner to a third party without the prior written consent of Philips Product Security and Services Office (PSSO).

Printed copies are uncontrolled unless authenticated.



### Case2:

Old POC:

1. Configure your browser to use a proxy tool such as Burp.
  2. Log in to the forcare admin application as user without SYSTEM\_PHI\_READ.
  3. It is observed that the user without SYSTEM\_PHI\_READ role defined can view/read the following api endpoints which consists of sensitive information like, backend components/versions, encryption password etc.

### **Supportive Evidence:**

PHILIPS SCOE

Confidential



This document is proprietary and confidential. No part of this document may be disclosed in any manner to a third party without the prior written consent of Philips Product Security and Services Office (PSSO).

Printed copies are uncontrolled unless authenticated.



A user with SYSTEM\_PHI\_READ has view option on backend configuration which includes sensitive information.

Send Cancel < > Target: https://ec2-3-70-166-239.eu-central-1.compute.amazonaws.com

Request		Response				Inspector
Pretty	Raw	Hex	Pretty	Raw	Hex	Selection
1 GET /admin/services/admin/components/admin/status/retrieve.js onformat=true HTTP/1.1	1	834 {	834 "key": "package.access",	2 Host: ec2-3-70-166-239.eu-central-1.compute.amazonaws.com	835 "value":	835 "sun.org.apache.catalina.,org.apache.coyote.,
2 Cookie: JSESSIONID=BAlA55128FOACF1440AA05EC6336A2E	2	836 "org.apache.jasper.,org.apache.tomcat."	836 },	3 Sec-Ch-Ua: "Chromium";v="109", "Not_A_Brand";v="99"	837 },	837 {
3 Sec-Ch-Ua: "Chromium";v="109", "Not_A_Brand";v="99"	3	838 "key": "server.loader",	838 "value": ""	4 Sec-Ch-Ua: "AppleWebKit/537.36 (KHTML, like Gecko)"	839 },	839 },
4 Sec-Ch-Ua: "AppleWebKit/537.36 (KHTML, like Gecko)"	4	840 "key": "",	840 "value": ""	5 Content-Type: application/x-www-form-urlencoded	841 },	841 {
5 Content-Type: application/x-www-form-urlencoded	5	842 "key": "forcare.passwordEncryptionKeyStorePassword",	842 "value": "forcare"	6 X-Requested-With: XMLHttpRequest	843 },	843 },
6 X-Requested-With: XMLHttpRequest	6	844 "key": "forcare.passwordEncryptionKeyStoreUrl",	844 "value": "file:/usr/local/forcare/certificates/password	7 Sec-Ch-Ua: "Mobile: 70"	845 },	845 encryption.p12"
7 Sec-Ch-Ua: "Mobile: 70"	7	846 },	846 },	8 Sec-Ch-Ua: "Windows"	847 },	847 {
8 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64)	8	848 "key": "forcare.configproperties.ISPtls",	848 "value": "false"	9 Sec-Ch-Ua: "Windows"	849 },	849 },
9 Sec-Ch-Ua: "Windows"	9	850 },	850 },	10 Accept: */*	851 },	851 },
10 Accept: */*	10	852 },	852 },	11 Sec-Fetch-Site: same-origin	853 },	853 },
11 Sec-Fetch-Site: same-origin	11			12 Sec-Fetch-Mode: cors		
12 Sec-Fetch-Mode: cors	12			13 Sec-Fetch-Dest: empty		
13 Sec-Fetch-Dest: empty	13			14 Referer:		
14 Referer:	14			https://ec2-3-70-166-239.eu-central-1.compute.amazonaws.c		
https://ec2-3-70-166-239.eu-central-1.compute.amazonaws.c				om/admin/admin/overview.html		
om/admin/admin/overview.html				15 Accept-Encoding: gzip, deflate		
15 Accept-Encoding: gzip, deflate	15			16 Accept-Language: en-US,en;q=0.9		
16 Accept-Language: en-US,en;q=0.9	16			17 Connection: close		
17 Connection: close	17					

PHILIPS SCOE

Confidential



This document is proprietary and confidential. No part of this document may be disclosed in any manner to a third party without the prior written consent of Philips Product Security and Services Office (PSSO).

Printed copies are uncontrolled unless authenticated.



### 8.3 Webapp: Weak Password Policy

Vulnerability Title	Weak Password Policy
Vulnerability Category	A6 - Security Misconfiguration
Severity	Medium
CVSS V3 Calculation	CVSS Base Score: 4.6 CVSS:3.0/AV:A/AC:H/PR:H/UI:R/S:U/C:L/I:H/A:N
Description	<p><b><u>Vulnerability Description:</u></b></p> <p>The application does not enforce a strong password policy to prevent malicious users from manually guessing or brute-forcing legitimate account passwords. Weak password policies include those that allow passwords consisting of common dictionary words, commonly-used passwords (For example., 1234), passwords that contain the associated username, sequential characters, and passwords shorter than 9 characters. By allowing users to create easily-guessable passwords, an attacker with minimal knowledge of registered users and username formats could crack passwords through the use of any of several techniques. In an online attack, an attacker can use consecutive login attempts to determine simple passwords. In an offline attack (For eaxmple., if the attacker has gained access to the raw contents of the password database through some other means), the attacker can employ richer techniques such as pre-computed hash attacks, free of rate-limiting and account-locking protections that might be employed against online password brute-forcing attacks.</p> <p><b>Retest (05-Jun-2023):</b> It is observed that the issue persists.</p> <p><b>Retest (31-Jan-2023):</b> It is observed that just like previous time there is no password policy in place, even password of single character is accepted.</p> <p><b><u>Exploitability rational</u></b></p> <p>Weak passwords may be easily guessed. This increases the likelihood a user's account may be compromised by an attacker. Once compromised, an attacker can have full access to the victim's account, potentially including the ability to modify settings, features and passwords. If the target account holds</p>

PHILIPS SCOE



Confidential

This document is proprietary and confidential. No part of this document may be disclosed in any manner to a third party without the prior written consent of Philips Product Security and Services Office (PSSO).



Printed copies are uncontrolled unless authenticated.



	<p>administrative privileges, the attacker can modify data for other users and/or the entire system</p> <p><b>Impact rational:</b> Credentials can be easily brute force. . Due to the prevalence of password reuse, a compromised password may also provide an attacker with credentials that can be used to attack other systems the victim uses the same credentials to access.</p>
<b>Affected Systems/IP Address/URL</b>	<p>Retest (05-Jun-2023):</p> <p><a href="https://server_url/admin/">https://server_url/admin/</a></p> <p><a href="https://server_url/audit/">https://server_url/audit/</a></p> <p><a href="https://server_url/viewer/">https://server_url/viewer/</a></p> <p>Old:</p> <p><a href="https://ec2-3-70-166-239.eu-central-1.compute.amazonaws.com/admin/">https://ec2-3-70-166-239.eu-central-1.compute.amazonaws.com/admin/</a></p> <p><a href="https://ec2-3-70-166-239.eu-central-1.compute.amazonaws.com/audit/">https://ec2-3-70-166-239.eu-central-1.compute.amazonaws.com/audit/</a></p> <p><a href="https://ec2-3-70-166-239.eu-central-1.compute.amazonaws.com/viewer/">https://ec2-3-70-166-239.eu-central-1.compute.amazonaws.com/viewer/</a></p>
<b>Recommendation</b>	<p><b>Recommendation:</b></p> <p>Implement a strong password complexity policy. A strong password policy is one which combines rules to prevent easily-guessable passwords from being used while also ensuring that passwords contain sufficient entropy. A password policy which provides a large set of restrictions can ultimately result in a smaller potential pool of passwords, lowering the amount of time necessary to guess a password through brute-force attacks. Conversely, an overly permissive policy allows users to create easily-guessable passwords. Put constraints in place to prevent users from choosing easily-guessable passwords at the time of creation, specifically those that are targeted by well-known dictionary attacks. This can minimize the likelihood that an attack may be successful if an attacker attempts to guess commonly-used passwords or employs an automated dictionary attack against a particular user.</p>



In the event that company policy does not stipulate password requirements, or the existing requirements are weak, consider employing the following password complexity requirements:

- Passwords must be at least nine (9) characters long.
- Passwords must contain some combination of at least three (3) of the following classes of characters: lowercase, uppercase, numeric, and “special” (For example., !, @, #, \$, %, ^, etc.) characters.
- Passwords should not be a dictionary word in any language, slang, dialect, jargon, etc.
- Passwords should not be based on personal information, etc.

## Status

**Open**

## Steps to Reproduce

**Retest (05-Jun-2023):**

The screenshot shows a browser's developer tools Network tab with a single captured request and response. The request is a POST to `/admin/services/user/add`. The response is a 200 OK status with the following headers:

```

HTTP/1.1 200 OK
Cache-Control: no-store, no-cache, must-revalidate
Content-Type: application/json; charset=UTF-8
Content-Length: 118
Date: Tue, 06 Jun 2023 11:15:37 GMT
Etag: "0"
Expires: 0
Forcet.com-Logcontext: f90178012124/admin-10B04
X-Content-Type-Options: nosniff
X-Frame-Options: SAMEORIGIN
X-Xss-Protection: 1; mode=block
Connection: close
    
```

The response body contains a JSON object with several fields, including `id`, `name`, `email`, `password`, `teamName`, `teamId`, `postalAddress`, `phoneNumbers`, `email2`, `preferredLanguage`, and `role`.

## Old POC:

Weak password accepted for add user feature in ForAdmin portal.

PHILIPS SCOE

Confidential

This document is proprietary and confidential. No part of this document may be disclosed in any manner to a third party without the prior written consent of Philips Product Security and Services Office (PSSO).



Printed copies are uncontrolled unless authenticated.



Target: <https://ec2-3-70-166-239.eu-central-1.compute.amazonaws.com>

Request	Response	Inspector
<pre>Pretty Raw Hex 1 POST /admin/services/user/add HTTP/1.1 2 Host: ec2-3-70-166-239.eu-central-1.compute.amazonaws.com 3 Cookie: JSESSIONID=13E603293D34C9973F236EA861CCCE66 4 Content-Length: 276 5 Sec-Ch-Ua: "Chromium";v="109", "Not_A Brand";v="99" 6 X-Forcare-Challenge: [[REDACTED]] 7 Sec-Ch-Ua-Mobile: 70 8 Authorization: Bearer [[REDACTED]] 9 Connection: close 10 11 uid=lmail+14401.com&amp;givenName=a&amp;sn=a&amp;cn=a&amp;postalAddress -a[UserPassword=&amp;#03d=Hestia@0General%20Practitioners&amp;ou= Hestia@0General%20Practitioners&amp;organizationUid= hestia.general.practitioners&amp;telephoneNumber=&amp;mobile=&amp; pager=&amp;registeredAddress=&amp;title=&amp;initials=&amp; preferredLanguage=</pre>	<pre>Pretty Raw Hex Render 1 HTTP/1.1 200 OK 2 Cache-Control: no-store, no-cache, must-revalidate 3 Cache-Control: post-check=0, pre-check=0 4 Content-Length: 0 5 Content-Type: application/octet-stream 6 Date: Mon, 30 Jan 2023 06:21:45 GMT 7 Expires: 0 8 Forcare.com-Logcontext: f90178012241/admin-573280 9 X-Content-Type-Options: nosniff 10 X-Frame-Options: SAMEORIGIN 11 X-Xss-Protection: 1; mode=block 12 Connection: close 13 14</pre>	<a href="#">Request Attributes</a> <a href="#">Request Query Parameters</a> <a href="#">Request Body Parameters</a> <a href="#">Request Cookies</a> <a href="#">Request Headers</a> <a href="#">Response Headers</a>

Weak login password for the portals.

Target: <https://ec2-3-70-166-239.eu-central-1.compute.amazonaws.com>

Request	Response	Inspector
<pre>Pretty Raw Hex 1 POST /admin/services/user/login.json HTTP/1.1 2 Host: ec2-3-70-166-239.eu-central-1.compute.amazonaws.com 3 Cookie: JSESSIONID=417e9f4b5aae39a05f36dbfc2b54d5aa 4 Content-Length: 31 5 Sec-Ch-Ua: "Chromium";v="109", "Not_A Brand";v="99" 6 Content-Type: application/x-www-form-urlencoded 7 X-Requested-With: XMLHttpRequest 8 Sec-Ch-Ua-Mobile: 70 9 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/109.0.5414.75 Safari/537.36 10 11 j_username=root&amp;j_password=root</pre>	<pre>Pretty Raw Hex Render 1 HTTP/1.1 200 OK 2 Cache-Control: no-store, no-cache, must-revalidate 3 Cache-Control: post-check=0, pre-check=0 4 Content-Length: 1103 5 Content-Type: application/json;charset=UTF-8 6 Date: Mon, 30 Jan 2023 06:23:53 GMT 7 Expires: 0 8 Forcare.com-Logcontext: f90178012241/admin-573290 9 Set-Cookie: JSESSIONID=B19FE1C03008C9C5BCF25D19791FA295; Path=/admin; Secure; HttpOnly; SameSite=Lax 10 X-Content-Type-Options: nosniff 11 X-Frame-Options: SAMEORIGIN 12 X-Xss-Protection: 1; mode=block 13 Connection: close 14 15 {   "response":{     "status":"ok",   } }</pre>	<a href="#">Request Attributes</a> <a href="#">Request Query Parameters</a> <a href="#">Request Body Parameters</a> <a href="#">Request Cookies</a> <a href="#">Request Headers</a> <a href="#">Response Headers</a>

PHILIPS SCOE



Confidential

This document is proprietary and confidential. No part of this document may be disclosed in any manner to a third party without the prior written consent of Philips Product Security and Services Office (PSSO).



Printed copies are uncontrolled unless authenticated.



## 8.4 Webapp: DOM Cross-Site Scripting (XSS)

Vulnerability Title	DOM Cross-Site Scripting (XSS)
Vulnerability Category	A3- Injection
Severity	Low
CVSS V3 Calculation	CVSS Base Score: 3.5 CVSS:3.0/AV:N/AC:L/PR:L/UI:R/S:U/C:L/I:N/A:N
Description	<p><b>Vulnerability Description:</b> During the security assessment it is observed that the application is vulnerable to DOM XSS attack.</p> <p>DOM based XSS is an XSS attack wherein the attack payload is executed as a result of modifying the DOM “environment” in the victim’s browser used by the original client side script, so that the client side code runs in an “unexpected” manner. That is, the page itself (the HTTP response that is) does not change, but the client side code contained in the page executes differently due to the malicious modifications that have occurred in the DOM environment.</p> <p><b>Retest (03-Jun-2023):</b> During the retest, it is observed that the issue persists.</p> <p>Reducing the severity to low as XSS is no more happening.</p> <p><b>Retest (31-Jan-2023):</b> It is identified that DOM based XSS payload uncaught exception error indicating fix is not properly implemented yet.</p> <p><b>Exploitability Rational:</b> For a successful exploitation of the issue, the victim should not be logged in to the application.</p> <p><b>Impact Rational:</b> DOM Cross-Site Scripting vulnerabilities give the attacker control of HTML and JavaScript running the user’s browser. The attack can alter page content with malicious HTML or JavaScript code. The attacker can arbitrarily alter page content displayed to the victim and can execute application functions using the victim’s application identity if the victim is authenticated to the application.</p>

PHILIPS SCOE



Confidential

This document is proprietary and confidential. No part of this document may be disclosed in any manner to a third party without the prior written consent of Philips Product Security and Services Office (PSSO).



Printed copies are uncontrolled unless authenticated.



<b>Affected Systems/IP Address/URL</b>	<p>Retest (03-Jun-2023):</p> <p><a href="https://server_url/viewer/document/list.html?patientID=%3Cimg/src%3dx%20onerror%3dalert(document.URL)%3E%5E%5E%261.3.6.1.4.1.21367.2005.3.7%26ISO">https://server_url/viewer/document/list.html?patientID=%3Cimg/src%3dx%20onerror%3dalert(document.URL)%3E%5E%5E%261.3.6.1.4.1.21367.2005.3.7%26ISO</a></p> <p>Old:</p> <p><a href="https://ec2-3-70-166-239.eu-central-1.compute.amazonaws.com/viewer/document/list.html?patientID=%3Cimg/src%3dx%20onerror%3dalert(document.URL)%3E%5E%5E%261.3.6.1.4.1.21367.2005.3.7%26ISO">https://ec2-3-70-166-239.eu-central-1.compute.amazonaws.com/viewer/document/list.html?patientID=%3Cimg/src%3dx%20onerror%3dalert(document.URL)%3E%5E%5E%261.3.6.1.4.1.21367.2005.3.7%26ISO</a></p>
<b>Recommendation</b>	<p>It is recommended to have proper input validation, also checking syntax-semantic (For example, a name field allowing special chars, number field accepting anything other than numeric digits., or allowing custom URL schema).</p> <p>Validation at Server side is required, you can bypass client side within javascript.</p> <p>Encode the output with Encoder.encodeForHTML and Encoder.encodeForJS before making dynamic updates to HTML.</p> <p>Considering any form of user input as untrusted and sanitizing it before operating anywhere.</p> <p>Avoid methods such as document.innerHTML and instead use safer functions, for example, document.innerText and document.textContent. If you can, entirely avoid using user input, especially if it affects DOM elements such as the document.url, the document.location, or the document.referrer.</p>
<b>Status</b>	<b>OPEN</b>

#### Supportive evidence (03-Jun-2023):

PHILIPS SCOE



Confidential

This document is proprietary and confidential. No part of this document may be disclosed in any manner to a third party without the prior written consent of Philips Product Security and Services Office (PSSO).





## **Supportive evidences:**

**Payload:** <img/src%3dx%20onerror%3dalert(document.URL)>

A screenshot of a Microsoft Edge browser window. The address bar shows a URL: https://modern-cougar.aws.pentest forcarelabs.com/viewer/document/list.html?patientID=<img%20src%3d' onerror=alert(document.URL)%3E%5E%5E%5E%26ISO. A red box highlights this URL. Below the address bar, a dark gray warning dialog box is centered. It contains a logo of a person with a plus sign, the text "modern-cougar.aws.pentest forcarelabs.com", and a long URL starting with "https://modern-cougar.aws.pentest forcarelabs.com/viewer/document/list.html?patientID=<img%20src%3d' onerror=alert(document.URL)%3E%5E%5E%5E%26ISO". At the bottom right of the dialog is a blue "OK" button. The entire dialog is surrounded by a red border.

## Retest (31-Jan-2023):

Throws uncaught exception error which indicates the fix is not implemented properly.

PHILIPS SCOE

Confidential

This document is proprietary and confidential. No part of this document may be disclosed in any manner to a third party without the prior written consent of Philips Product Security and Services Office (PSSO).



Screenshot of the HealthSuite Interoperability Viewer showing a security error. The URL is https://ec2-3-70-166-239.eu-central-1.compute.amazonaws.com/viewer/document/list.html?patientID=<img/src%3dx%20onerror%3daler... . The page displays a 'Something went wrong' message with a red X icon. The error message is: n!forcare.xds.util.XdsException: ERROR; errorCode: XDSRegistryMetadataError; codeContext: metadata error (registry): Could not parse the request. Reason: cannot parse patient ID: &lt;img/src=x onerror=alert(document.URL)&gt; (&lt;img/src=x onerror=alert(document.URL)&gt;)^~^&lt;1.3.6.1.4.1.21367.2005.3.7&ISO: is not a valid patient ID in XDS; form should be id^^^&authority&ISO.; location: ParserUtil.handleMetadataError . An 'OK' button is at the bottom right of the error dialog.

PHILIPS SCOE



Confidential

This document is proprietary and confidential. No part of this document may be disclosed in any manner to a third party without the prior written consent of Philips Product Security and Services Office (PSSO).



Printed copies are uncontrolled unless authenticated.



## 8.5 Webapp: Weak Input Validation

Vulnerability Title	Weak Input Validation
Vulnerability Category	A3 - Injection
Severity	Low
CVSS V3 Calculation	CVSS Base Score: 3.1 CVSS:3.0/AV:N/AC:H/PR:H/UI:R/S:U/C:N/I:L/A:L
Description	<p><b>Vulnerability Description:</b> During the assessment it is observed that the application stores or processes untrusted data that is not sufficiently validated. This may be due to a complete lack of validation or validation filters whose implementation does not provide sufficient protection for the given input. An application may obtain data from various external and internal sources including databases, file servers, web services, external client requests, etc. While some of these sources may be considered trustworthy, no assumptions should be made about the validity of data whose source cannot be explicitly verified. This includes not only external data, but also data that was previously stored by the same application and data generated by other entities in the same organization.</p> <p><b>Retest (06-Jun-2023):</b> It is identified that the issue persists.</p> <p><b>Retest (31-Jan-2023):</b> It is identified that the issue is still same like previous time.</p> <p><b>Exploitability Rational:</b> Failure to properly validate and handle untrusted input represents the single largest category of software security weaknesses. At a minimum, data that is not validated may impact the application's control flow or data flow, leading to unexpected application states for end users, unintended changes to back-end data, as well as unexpected outcomes from executed application logic.</p> <p>An attacker may submit payloads that seek to exploit any number of vulnerabilities that typically result from a lack of input validation. These include (but are not limited to) SQL injection, cross-site scripting, LDAP injection, log injection, and command injection. The consequence of successfully exploiting these vulnerabilities varies, but most provide an attacker with the ability to bypass authentication and/or authorization mechanisms to access, modify or</p>

PHILIPS SCOE



Confidential

This document is proprietary and confidential. No part of this document may be disclosed in any manner to a third party without the prior written consent of Philips Product Security and Services Office (PSSO).



Printed copies are uncontrolled unless authenticated.



	<p>delete application and user data, or execute functionality only available to legitimate users.</p> <p><b>Impact Rational:</b> An attacker can provide unexpected values and cause a program crash or excessive consumption of resources, such as memory and CPU. An attacker can read confidential data if they can control resource references. An attacker can use malicious input to modify data or possibly alter control flow in unexpected ways, including arbitrary command execution.</p>
Affected Systems/IP Address/URL	<p>Retest (06-Jun-2023):</p> <p><a href="https://server_url/admin/">https://server_url/admin/</a></p> <p><a href="https://server_url/viewer/">https://server_url/viewer/</a></p> <p>Old:</p> <p><a href="https://ec2-3-70-166-239.eu-central-1.compute.amazonaws.com/viewer/">https://ec2-3-70-166-239.eu-central-1.compute.amazonaws.com/viewer/</a></p> <p><a href="https://ec2-3-70-166-239.eu-central-1.compute.amazonaws.com/admin/">https://ec2-3-70-166-239.eu-central-1.compute.amazonaws.com/admin/</a></p>
Recommendation	<p>We recommend the following:</p> <ul style="list-style-type: none"> <li>• Data that does not match an expected pattern and data that can potentially be used to execute injection attacks must be discarded or sanitized before use.</li> <li>• Perform the validation in such a way that end-users cannot tamper with or bypass the control. Perform the validation on the server-side rather than client-side.</li> </ul> <p>Whitelist validation should be favored first over other validation techniques since any character or string not explicitly specified as part of the "known-safe" set of characters or values is rejected or removed by default.</p>
Status	Open

### Supportive evidence

Retest (06-Jun-2023):

PHILIPS SCOE



Confidential

This document is proprietary and confidential. No part of this document may be disclosed in any manner to a third party without the prior written consent of Philips Product Security and Services Office (PSSO).



<https://3.71.200.223/viewer/patient/query.html#/0/document/container:medicalDocuments/patientId=<h1>myID<%2Fh1>%5E%5E%5E%261.3.6.1.4.1.21367.2005.3.7%26ISO>

HealthSuite Interoperability Viewer

Home > Patient Search > Patient Record > Medical Documents

<h1>lastName</h1>, <h1>givenName</h1>	ID: <h1>myID</h1> (HOS)	Aug 9, 2010 (12 yr)	Male
Address <h1>Street</h1>, <h1>postalcode</h1> <h1>resident</h1>	Phone -		

Filter results: No documents | Change purpose of use

Creation Date ▾ Title ▾ Author ▾ Author Role ▾ Author Institution ▾ Author IP ▾

### Old POC:

<https://ec2-3-70-166-239.eu-central-1.compute.amazonaws.com/viewer/patient/query.html#/0/document/container:medicalDocuments/patientId=<h1>pentest</h1>, <h1>pentest</h1>>

HealthSuite Interoperability Viewer

Home > Patient Search > Patient Record > Medical Documents

<h1>pentest</h1>, <h1>pentest</h1>	ID: 102 (HOS)	Jan 1, 2022 (1 yr)	Male
Address <h1>pentest</h1>, <h1>pentest</h1> <h1>pentest</h1>	Phone -	Email -	

Medical Documents Referrals Patient Consent Patient Details Exports

Show deprecated documents | Add a document

Filter results: No documents | Change purpose of use

Creation Date ▾ Title ▾ Author ▾ Author Role ▾ Author Institution ▾ Type ▾

PHILIPS SCOE



Confidential

This document is proprietary and confidential. No part of this document may be disclosed in any manner to a third party without the prior written consent of Philips Product Security and Services Office (PSSO).



Printed copies are uncontrolled unless authenticated.



## 8.6 Webapp: Improper Error & Exception Handling

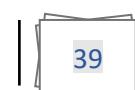
Vulnerability Title	Improper Error & Exception Handling
Vulnerability Category	A6 - Security Misconfiguration
Severity	Low
CVSS V3 Calculation	CVSS Base Score: 3.7 CVSS v3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:L/I:N/A:N
Description	<p><b>Vulnerability Description:</b> it is observed that the web application reveals sensitive information as part of its error messages such as stack trace, server versions, name of server-side parameter.</p> <p><b>Retest (06-Jun-2023):</b> It is identified that the issue persists.</p> <p><b>Retest (31-Jan-2023):</b> It is identified that same like previous time, errors are displayed to the end user.</p> <p><b>Exploitability Rational:</b> An attacker does not require authentication to the platform in order to leverage this vulnerability.</p> <p><b>Impact Rational:</b> Attackers may use this vulnerability to gain more information about the system before attempting to attack the web application.</p>
Affected Systems/IP Address/URL	<p>Retest (06-Jun-2023):</p> <p><a href="https://server_url/admin/">https://server_url/admin/</a></p> <p><a href="https://server_url/audit/">https://server_url/audit/</a></p> <p><a href="https://server_url/viewer/">https://server_url/viewer/</a></p> <p>Old:</p> <p><a href="https://ec2-3-70-166-239.eu-central-1.compute.amazonaws.com /viewer">https://ec2-3-70-166-239.eu-central-1.compute.amazonaws.com /viewer</a></p> <p><a href="https://ec2-3-70-166-239.eu-central-1.compute.amazonaws.com /admin">https://ec2-3-70-166-239.eu-central-1.compute.amazonaws.com /admin</a></p> <p><a href="https://ec2-3-70-166-239.eu-central-1.compute.amazonaws.com /audit">https://ec2-3-70-166-239.eu-central-1.compute.amazonaws.com /audit/</a></p>

PHILIPS SCOE



Confidential

This document is proprietary and confidential. No part of this document may be disclosed in any manner to a third party without the prior written consent of Philips Product Security and Services Office (PSSO).



Printed copies are uncontrolled unless authenticated.



<b>Recommendation</b>	It is recommended to Implement a mechanism to handle and log all errors that pull out the exception stack trace message. It is also recommended to display a generic error message instead of the stack trace.
<b>Status</b>	<b>Open</b>

## Supportive evidences

## **Retest (06-Jun-2023):**

Old:

## Improper error and exception as part of server response.

PHILIPS SCOF

Confidential

This document is proprietary and confidential. No part of this document may be disclosed in any manner to a third party without the prior written consent of Philips Product Security and Services Office (PSSO).



Target: <https://ec2-3-70-166-239.eu-central-1.compute.amazonaws.com>

**Request**

```
Pretty Raw Hex
1 POST /audit/services/audit/list.csv HTTP/1.1
2 Host: ec2-3-70-166-239.eu-central-1.compute.amazonaws.com
3 Cookie: center_bottom=; JSESSIONID=0177BEB134BC448D95F444F5B3ACDB
4 Sec-Ch-Ua: "Chromium";v="109", "Not_A Brand";v="99"
5 Sec-Ch-Ua-Mobile: 70
6 Sec-Ch-Ua-Platform: "Windows"
7 Upgrade-Insecure-Requests: 1
8 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/109.0.5414.75 Safari/537.36
9 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9
10 Sec-Fetch-Site: same-origin
11 Sec-Fetch-Mode: navigate
12 Sec-Fetch-User: ?1
13 Sec-Fetch-Dest: iframe
14 Referer: https://ec2-3-70-166-239.eu-central-1.compute.amazonaws.com/audit/index.html
15 Accept-Encoding: gzip, deflate
16 Accept-Language: en-US,en;q=0.9
```

**Response**

```
Pretty Raw Hex Render
1 HTTP/1.1 405 Method Not Allowed
2 Content-Type: text/xml;charset=UTF-8
3 Date: Mon, 30 Jan 2023 09:18:27 GMT
4 Forcare.com-Logcontext: a8ac29a0a030/audit-119391
5 Vary: accept-encoding
6 X-Content-Type-Options: nosniff
7 X-Frame-Options: SAMEORIGIN
8 X-Xss-Protection: 1; mode=block
9 Content-Length: 6032
10 Connection: close
11
12 <error message="POST method not allowed for path /services/audit/list.csv" logContextId="a8ac29a0a030/audit-119391" origin="/audit/services/audit/list.csv">
13   <cause>nl.forcare.common.servlet.HttpErrorException: POST method not allowed for path /services/audit/list.csv
14   </cause>
15   </causes>
16   <stacktrace>
nl.forcare.common.servlet.HttpErrorException: POST method not allowed for path /services/audit/list.csv
17   at nl.forcare.frontcontroller.MappingUrlMapper.createHandler
```

Target: <https://ec2-3-70-166-239.eu-central-1.compute.amazonaws.com>

**Request**

```
Pretty Raw Hex
1 GET /admin/services/admin/queue/retrieve.json?id=>
```

**Response**

```
Pretty Raw Hex Render
16 org.apache.tomcat.util.net.SocketProcessorBase.run(SocketProcessorBase.java:49)
17 org.apache.tomcat.util.threads.ThreadPoolExecutor$unWorker(ThreadPoolExecutor.java:1191)
18 org.apache.tomcat.util.threads.ThreadPoolExecutor$Worker.run(ThreadPoolExecutor.java:659)
19 org.apache.tomcat.util.threads.TaskThread$WrappingRunnable.run(TaskThread.java:61)
20 java.lang.Thread.run(Thread.java:750)
</pre>
<p>
  <b>Note</b>
  The full stack trace of the root cause is available in the server logs.
</p>
<hr class="line" />
<h3> Apache Tomcat/9.0.68 </h3>
</body>
```

PHILIPS SCOE

Confidential

This document is proprietary and confidential. No part of this document may be disclosed in any manner to a third party without the prior written consent of Philips Product Security and Services Office (PSSO).



## 8.7 Webapp: Sensitive Information in the URL

Vulnerability Title	Sensitive Information in the URL
Vulnerability Category	A6 - Security Misconfiguration
Severity	Low
CVSS V3 Calculation	CVSS Base Score: 3.1 CVSS:3.0/AV:N/AC:H/PR:L/UI:N/S:U/C:L/I:N/A:N
Description	<p><b>Vulnerability Description:</b> During the security assessment, it is observed that Sensitive information is exposed in via URL query string parameters. Username, PatientID, userID, Code are exposed via URL parameters. URLs may be stored or viewed in multiple places during and after a request is made to the server:</p> <ul style="list-style-type: none"> <li>URLs are often logged in multiple places including the browser history, proxy logs, and web server logs.</li> <li>The query string will be sent as part of the URL if the URL is passed to another site via the Referrer header.</li> <li>URLs sent to the user as part of an HTML page may be cached on disk.</li> </ul> <p><b>Retest (06-Jun-2022):</b> During the retest, it is identified that the URL still contains sensitive information.</p> <p><b>Retest (31-Jan-2022):</b> It is identified that the URL still contains sensitive information.</p> <p><b>Exploitability Rational:</b></p> <p>Potential access vectors may include, but are not limited to:</p> <ul style="list-style-type: none"> <li>Browser history, proxy logs, web server logs, etc.</li> <li>Utilizing other attacks (such as cross-site scripting) to extract sensitive information from the source of a page containing links to URLs with sensitive information in the query string</li> <li>Shoulder-surfing the URL in a user's browser address bar.</li> </ul>

PHILIPS SCOE



Confidential

This document is proprietary and confidential. No part of this document may be disclosed in any manner to a third party without the prior written consent of Philips Product Security and Services Office (PSSO).



Printed copies are uncontrolled unless authenticated.



	<p><b>Impact Rational:</b> Attacker who gains access to any location where URLs are stored can view sensitive information passed via the query string. Depending on the nature of the information, a malicious user may obtain personally identifiable information (PII), private user data or information which would allow user impersonation (in the event of credential or session identifier).</p>
Affected Systems/IP Address/URL	<p>Retest (06-Jun-2023):</p> <p><a href="https://server_url/viewer/services/document/list.json?patientIDAuth=&lt;Auth_ID&gt;&amp;patientID=&lt;PatientID&gt;">https://server_url/viewer/services/document/list.json?patientIDAuth=&lt;Auth_ID&gt;&amp;patientID=&lt;PatientID&gt;</a></p> <p>Old:</p> <p><a href="https://ec2-3-70-166-239.eu-central-1.compute.amazonaws.com/viewer/services/document/list.json?patientIDAuth=1.3.6.1.4.1.21367.2005.3.7&amp;patientID=134442134">https://ec2-3-70-166-239.eu-central-1.compute.amazonaws.com/viewer/services/document/list.json?patientIDAuth=1.3.6.1.4.1.21367.2005.3.7&amp;patientID=134442134</a></p>
Recommendation	Do not pass the sensitive data like credentials, UserID, codes or sessionIDs between the client and server via URL query string parameters.
Status	Open

## Steps to Reproduce

### Retest (06-Jun-2023):

Steps are same as before.

Screenshot of a browser developer tools Network tab showing three requests (7973, 7972, 7971) and their corresponding responses. The requests are GET requests to /viewer/services/document/list.json with various parameters. The responses show JSON data, including a 'result' field with a large base64 encoded string.

Request	Response
7973 https://3.71.200.223	Pretty Raw Hex Render
7972 https://3.71.200.223	Pretty Raw Hex Render
7971 https://3.71.200.223	Pretty Raw Hex Render

```

Request:
GET /viewer/services/document/list.json?patientIDAuth=1.3.6.1.4.1.21367.2005.3.7 HTTP/1.1
Host: 3.71.200.223
Cookie: JSESSIONID=DA8444661E10B8BA7AF625A16F5F0
Sec-Ch-Ua: "Not A Brand";v="100"
Content-Type: application/x-www-form-urlencoded
X-Requested-With: XMLHttpRequest
Sec-Ch-Ua-Mobile: ?0
Accept: */*
Accept-Language: en-US,en;q=0.5
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/114.0.5735.91 Safari/537.36
Sec-Ch-Ua-Platform: "Windows"
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: cors
Sec-Fetch-Dest: document
Referer: https://3.71.200.223/viewer/patient/query.html
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.5
Connection: close
200
200
200

Response:
HTTP/1.1 200 OK
Cache-Control: no-store, no-cache, must-revalidate
Content-Control: post-check=0, pre-check=0
Content-Type: application/json; charset=UTF-8
Date: Tue, 06 Jun 2023 13:23:27 GMT
Expires: -1
Server: tomcat
X-Frame-Context: 79a@f001e495/viewer-4350
Vary: accept-encoding
X-Content-Type-Options: nosniff
X-Frame-Options: SAMEORIGIN
X-Xss-Protection: 1; mode=block
Content-Length: 9996
Connection: close
14
1
{
  "result": {
    "warnings": [
      ...
    ],
    "documents": [
      {
        "nameType": "application/pdf",
        "id": "fc378770-ecc9-4b6e-beaf-74e1237d8f59",
        "logicalId": "fc378770-ecc9-4b6e-beaf-74e1237d8f59",
        "status": "Approved",
        "objectType": "ESTATE_DOCUMENT",
        "home": "1.2.3",
        "creationTime": "19940311",
        "lastModified": "20230619-027a5bc0cd17e410b3d57b526",
        "languageCode": "en-US",
        "serviceType": "ESTATE",
        "size": "64KB",
        "sourcePatientId": "134442134",
        "sourcePatientInfo": {
          "PID": "1-134442134",
          "PIS": "134442134",
          "PISID": "134442134",
          "PISN": "134442134",
          "PISL": "134442134",
          "PISU": "134442134"
        },
        "PIS": "134442134",
        "PISID": "134442134",
        "PISN": "134442134",
        "PISL": "134442134",
        "PISU": "134442134"
      }
    ]
  }
}
0 matches

```

PHILIPS SCOE

Confidential

This document is proprietary and confidential. No part of this document may be disclosed in any manner to a third party without the prior written consent of Philips Product Security and Services Office (PSSO).



## Old POC:

- Launch ForView Applications.
- Intercept the requests using Burp proxy tool.
- As observed in below request PatientID and PatientIDAuth value gets sent for GET requests, which can get logged.

Screenshot of the Burp Suite interface showing two captured HTTP requests. The first request is highlighted with a red box.

Request	Response
<pre>Pretty Raw Hex 1 GET /viewer/services/document/list.json?patientID= 7345342758955&amp;patientIDAuth= 1.3.e.1.4.1.21367.2005.3.7 HTTP/1.1 2 Host: ec2-3-70-166-239.eu-central-1.compute.amazonaws.com 3 Cookie: JSESSIONID=19E4C3E3306978427688E8F51FF56C97 4 Sec-Ch-Ua: "Chromium";v="109", "Not_A_Brand";v="99" 5 Content-Type: application/x-www-form-urlencoded 6 X-Requested-With: XMLHttpRequest 7 Sec-Ch-Ua-Mobile: ? 8 Authorization: Bearer eyJhbGciOiJSUzI1NiIiIngldCI6IjFLbmQtSER4eEgtZkZjeXl Xby1DTmpnOVVFcyJ9.eyJpc3M1oJ1cm46b21k0jEuM140IiwiY XVkijoiaHR0cHM6Ly9sb2NhbgHvc3Q6ODA4MS92aWV3ZXiiLCJz dWli0iJyb290IiwiU3ViamVjdE1Eijoicm9vdCisIdNhbmguaWN hbFvzZXJJZC16InVp2Diyb290LGRjPWRvbWFpbixkYz1sb2Nhbc IsI1N1Ymp1Y3RfPcmdhbmlfYXRpb24iOlsirXkhbXBsZSBPcmdhb ml6YXRpb24IXSwicm9sZXMiOlsiq2xpbm1jYWxBZGlpbmlzdHJh dG9ycyIsI1N5c3R1bUFkbWluaxXNOcmF0b3JzI10sI1N1Ymp1Y3R Sb2x1IjpbeYJjb2R1Ijo1Q2xpbm1jYWxBZGlpbmlzdHJhdG9ycy</pre>	<pre>Pretty Raw Hex Render 1 HTTP/1.1 200 OK 2 Cache-Control: no-store, no-cache, must-revalidate 3 Cache-Control: post-check=0, pre-check=0 4 Content-Type: application/json; charset=UTF-8 5 Date: Mon, 30 Jan 2023 06:10:10 GMT 6 Expires: 0 7 Forcare.com-Logcontext: 79a0f001e495/viewer-281391 8 Vary: accept-encoding 9 X-Content-Type-Options: nosniff 10 X-Frame-Options: SAMEORIGIN 11 X-Xss-Protection: 1; mode=block 12 Content-Length: 8127 13 Connection: close 14 15 {     "result": [         "warnings": [         ],         "documents": [         ]     ] }</pre>

PHILIPS SCOE

Confidential

This document is proprietary and confidential. No part of this document may be disclosed in any manner to a third party without the prior written consent of Philips Product Security and Services Office (PSSO).



## 8.8 Webapp: HTTP Strict Transport Security (HSTS) Not Implemented

Vulnerability Title	HTTP Strict Transport Security (HSTS) Not Implemented
Vulnerability Category	A6 - Security Misconfiguration
Severity	Low
CVSS V3 Calculation	CVSS Base Score: 3.8 CVSS:3.0/AV:L/AC:H/PR:H/UI:R/S:U/C:L/I:L/A:L
Description	<p><b><u>Vulnerability Description:</u></b></p> <p>The server does not implement the "HTTP Strict-Transport Security" (HSTS) web security policy mechanism. When HSTS is enabled, the web application sends a special response header, "Strict-Transport-Security" to the client with a duration of time specified. Once a supported browser receives this header, that browser can only make requests to the application over HTTPS for the duration of time specified in the header. Any links to resources over HTTP will be rewritten to HTTPS before the request is made.</p> <p><b>Retest (06-Jun-2023):</b> It is identified that the issue persists.</p> <p><b>Retest (31-Jan-2022):</b> It is identified that just like previous time issues is same.</p> <p><b><u>Exploitability rational</u></b></p> <p>Applications that do not utilize the "HTTP Strict-Transport Security" policy are more susceptible to man-in-the-middle attacks via SSL stripping, which occurs when an attacker transparently downgrades a victim's communication with the server from HTTPS to HTTP. Once this is accomplished, the attacker will gain the ability to view and potentially modify the victim's traffic, exposing sensitive information and gaining access to unauthorized functionality.</p> <p>Attacker can gain sensitive information and access for the unauthorized functionality.</p>

PHILIPS SCOE



Confidential

This document is proprietary and confidential. No part of this document may be disclosed in any manner to a third party without the prior written consent of Philips Product Security and Services Office (PSSO).



Printed copies are uncontrolled unless authenticated.



	<b>Impact rational:</b> Attacker can gain sensitive information and access for the unauthorized functionality.
Affected Systems/IP Address/URL	<p>Retest (06-Jun-2023):</p> <p><a href="https://server_url/admin/">https://server_url/admin/</a></p> <p><a href="https://server_url/audit/">https://server_url/audit/</a></p> <p><a href="https://server_url/viewer/">https://server_url/viewer/</a></p> <p><a href="https://server_url/imageupload/">https://server_url/imageupload/</a></p> <p>Old:</p> <p><a href="https://ec2-3-70-166-239.eu-central-1.compute.amazonaws.com/admin">https://ec2-3-70-166-239.eu-central-1.compute.amazonaws.com/admin</a></p> <p><a href="https://ec2-3-70-166-239.eu-central-1.compute.amazonaws.com/audit">https://ec2-3-70-166-239.eu-central-1.compute.amazonaws.com/audit</a></p> <p><a href="https://ec2-3-70-166-239.eu-central-1.compute.amazonaws.com/imageupload?assigningAuthority=1.3.6.1.4.1.21367.2005.3.7#/start">https://ec2-3-70-166-239.eu-central-1.compute.amazonaws.com/imageupload?assigningAuthority=1.3.6.1.4.1.21367.2005.3.7#/start</a></p> <p><a href="https://ec2-3-70-166-239.eu-central-1.compute.amazonaws.com/viewer">https://ec2-3-70-166-239.eu-central-1.compute.amazonaws.com/viewer</a></p>
Recommendation	<p>The application server should send the "Strict-Transport-Security" HTTP header in each response indicating that future requests to the domain use only HTTPS. The following is a basic example of the HSTS HTTP header, setting a max-age of one year:</p> <p>Strict-Transport-Security: max-age=31536000</p> <p>Subdomains should also be configured in this manner, by including the "includeSubDomains" flag:</p> <p>Strict-Transport-Security: max-age=31536000; includeSubDomains;</p>
Status	<b>Open</b>

### Steps to Reproduce

**Retest (06-Jun-2023):**

PHILIPS SCOE



Confidential

This document is proprietary and confidential. No part of this document may be disclosed in any manner to a third party without the prior written consent of Philips Product Security and Services Office (PSSO).



Printed copies are uncontrolled unless authenticated.



Intercept HTTP history WebSockets history ⚙️

Filter Not matching expression Strict-Transport-Security

#	Host	Method	URL	Params	Edited	Status code	Length	MIME type	Extension	Title	Comment	TLS	IP	Cookies	Time
7620	https://3.71.200.223	GET	/admin/services/organization/list.json			200	3647	JSON	json			✓	3.71.200.223		164104 6 Jun
7623	https://3.71.200.223	GET	/admin/services/user/filter?usernameFilter=			200	22532	JSON	json			✓	3.71.200.223		164104 6 Jun
7627	https://3.71.200.223	GET	/admin/2301-26/img/button/button.svg			200	2972	XML	svg			✓	3.71.200.223		164104 6 Jun
7628	https://3.71.200.223	GET	/admin/services/admin/components/index/status/retrieve.json?format=true			✓	200	1255458	JSON	json		✓	3.71.200.223		164104 6 Jun
7629	https://3.71.200.223	GET	/admin/services/admin/components/connect/status/retrieve.json?format=true			✓	200	114497	JSON	json		✓	3.71.200.223		164104 6 Jun
7624	https://3.71.200.223	GET	/admin/services/admin/components/cca/status/retrieve.json?format=true			✓	200	2384519	JSON	json		✓	3.71.200.223		164104 6 Jun
7623	https://3.71.200.223	GET	/admin/services/admin/components/audit/status/retrieve.json?format=true			✓	200	1337926	JSON	json		✓	3.71.200.223		164104 6 Jun
7622	https://3.71.200.223	GET	/admin/2301-26/img/toolbar/small-tuning.svg			200	1391	XML	svg			✓	3.71.200.223		164104 6 Jun

Request

Pretty Raw Hex

```
1 GET /admin/services/users/list.json?userNameFilter= HTTP/1.1
2 Host: 3.71.200.223
3 Cookie: JSESSIONID=177A11A3ADEF84B10C6109C71EDC6D0
4 Sec-Ch-Ua: "Chromium";v="105", "Not A Brand";v="99"
5 Content-Type: application/x-www-form-urlencoded
6 X-Requested-With: XMLHttpRequest
7 Sec-Ch-User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
8 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
9 Chrome/114.0.5735.91 Safari/537.36
10 Sec-Ch-User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
11 Sec-Fetch-User: none;origin=
12 Sec-Fetch-Dest: same-origin
13 Sec-Fetch-Mode: cors
14 Sec-Fetch-Dest: empty
15 Referer: https://3.71.200.223/admin/admin/overview.html
16 Accept-Encoding: gzip, deflate, br
17 Accept-Language: en-US,en;q=0.9
18 Connection: close
19
20
```

Response

Pretty Raw Hex Render

```
1 HTTP/1.1 200 OK
2 Cache-Control: no-store, no-cache, must-revalidate
3 Cache-Control: post-check=0, pre-check=0
4 Content-Type: application/json; charset=UTF-8
5 Date: Tue, 06 Jun 2023 11:11:00 GMT
6 Expires: 0
7 Forcare.com-Logcontext: f90178012241/admin-10757
8 Vary: accept-encoding
9 X-Content-Type-Options: nosniff
10 X-Frame-Options: SAMEORIGIN
11 X-Kss-Protection: 1; mode=block
12 Connection: close
13 Content-Length: 22114
14 {
  "result": {
    "complete": true,
    "persons": [
      {
        "dn": "uid=000012310,uid=000000381,ou=practices,ou=users,dc=forcare,dc=local",
        "uid": "00001230",
        "useEmail": "true",
        "mail": "test@forcare.com",
        "givenName": "Otto",
        "objectClass": [
          "top",
          "inetOrgPerson",
          "person",
          "organizationalPerson",
          "overseerPerson"
        ],
        "user": "test-00001230",
        "emp": "Otto test-00001230",
        "rnr": "1000000 Zorginstelling 01",
        "role": [
          {
            "department": ""
          }
        ],
        "dn": "uid=000012352,uid=000000381,ou=practices,ou=users,dc=forcare,dc=local",
        "user": "test-000012352"
      }
    ]
  }
}
```

Inspector

- Request attributes
- Request query parameters
- Request cookies
- Request headers
- Response headers

## Old:

2551 https://ec2-3-70-166-239.eu... GET /admin/services/admin/queue/retrieve.json 200 216208 JSON json

2548 https://ec2-3-70-166-239.eu... GET /admin/services/admin/components/list.json 200 1924 JSON json

Request

Pretty Raw Hex

```
1 GET /admin/services/admin/components/list.json
HTTP/1.1
2 Host:
ec2-3-70-166-239.eu-central-1.compute.amazonaws.com
3 Cookie: JSESSIONID=DEA7AD49BADDE1A7B8B177E13EB4539
4 Sec-Ch-Ua: "Chromium";v="105", "Not A Brand";v="99"
5 Content-Type: application/x-www-form-urlencoded
6 X-Requested-With: XMLHttpRequest
7 Sec-Ch-User-Agent: ?
8 Authorization: Bearer
eyJhbGciOiJSUzI1NiIsIngldCI6IjFLbmQtSER4eEgtZkZjeXl
Xby1DTmpnVVFCFcyJ9.eyJpc3MiOiJlcmt4b2lkOjEuM140IiwiY
XVkJjoiaHR0cHMlYsb2NhbGhv3Q6ODA4MS92aWV3ZXIIlCJz
dW10idjbz901iwiU3ViamVjdE1Ej0icm9vdCtsIkNhbmuaWN
hbFVzZKJJC16InVpZDiyb290LGRjPWRvbWPbjkxYzisb2NhbC
IsI1N1Tmp1Y3Rcmdhbm16YXRpb24iolsiRXhbXBsZSBPcmdhb
m16YXRpb24iXSwicms2XMIo1siQ2XpbmijYWxBZG1pbmizdHJh
dG9ycyisI1N5c3R1bUFkbWluaXN0cmfOb3JzI1OsI1N1Ymp1Y3R
Sb2x1IjpbeuyJjb2R1jjo1Q2xpbmijYWxBZG1pbmizdHjdG9ycy
Ie-TmNs-ZGUTeVNO7DQ1Lw-MuM4au-1CaMS4QMDM3MS4a-1-EwI
```

Response

Pretty Raw Hex Render

```
1 HTTP/1.1 200 OK
2 Cache-Control: no-store, no-cache, must-revalidate
3 Cache-Control: post-check=0, pre-check=0
4 Content-Length: 1529
5 Content-Type: application/json; charset=UTF-8
6 Date: Mon, 30 Jan 2023 06:47:30 GMT
7 Expires: 0
8 Forcare.com-Logcontext: f90178012241/admin-573864
9 X-Content-Type-Options: nosniff
10 X-Frame-Options: SAMEORIGIN
11 X-Kss-Protection: 1; mode=block
12 Connection: close
13
14 {
  "components": [
    {
      "id": "admin",
      "displayName": "forAdmin",
      "baseUrl": "https://localhost:8081/admin",
      "user": "test-00001230"
    }
  ]
}
```

Inspector

- Request Attributes
- Request Cookies
- Request Headers
- Response Headers

PHILIPS SCOE



Confidential

This document is proprietary and confidential. No part of this document may be disclosed in any manner to a third party without the prior written consent of Philips Product Security and Services Office (PSSO).



Printed copies are uncontrolled unless authenticated.



## 8.9 Webapp: No Account Lockout Policy

Vulnerability Title	No Account Lockout Policy
Vulnerability Category	A2 - Broken Authentication
Severity	Low
CVSS V3 Calculation	CVSS Base Score: 3.7 CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:N/A:L
Description	<p><b>Vulnerability Description:</b></p> <p>The application does not maintain or enforce an account lockout policy. A lockout policy refers to the mechanism that temporarily suspends a user's account after a certain number of unsuccessful authentication attempts have been made.</p> <p><b>Retest (06-Jun-2023):</b> It is identified that the issue persists.</p> <p><b>Retest (31-Jan-2022):</b> It is identified that just like previous time issues is same.</p> <p><b>Exploitability rational:</b> Applications with no lockout policy are vulnerable to brute force password guessing attacks, in which the attacker performs login attempts using a known username and a list of potential passwords until a successful combination is found. Once a successful combination is discovered, the attacker is granted full access to the compromised account, and can impersonate the victim without detection.</p> <p><b>Impact rational:</b> Without a strong lockout mechanism, the application can be susceptible to brute force attacks.</p>
Affected Systems/IP Address/URL	<p>Retest (06-Jun-2023):</p> <p><a href="https://server_url/admin/">https://server_url/admin/</a></p> <p><a href="https://server_url/audit/">https://server_url/audit/</a></p>

PHILIPS SCOE



Confidential

This document is proprietary and confidential. No part of this document may be disclosed in any manner to a third party without the prior written consent of Philips Product Security and Services Office (PSSO).



	<p><a href="https://server_url/viewer/">https://server_url/viewer/</a></p> <p>Old:</p> <p><a href="https://ec2-3-70-166-239.eu-central-1.compute.amazonaws.com/viewer/">https://ec2-3-70-166-239.eu-central-1.compute.amazonaws.com/viewer/</a></p> <p><a href="https://ec2-3-70-166-239.eu-central-1.compute.amazonaws.com/admin/">https://ec2-3-70-166-239.eu-central-1.compute.amazonaws.com/admin/</a></p> <p><a href="https://ec2-3-70-166-239.eu-central-1.compute.amazonaws.com/audit/">https://ec2-3-70-166-239.eu-central-1.compute.amazonaws.com/audit/</a></p>
<b>Recommendation</b>	It's recommended to implement some type of account lockout after a defined number of incorrect password attempts.
<b>Status</b>	<b>Open</b>

## Steps to Reproduce

Retest (06-Jun-2023):

Steps are same as before.

PHILIPS SCOE

Confidential

This document is proprietary and confidential. No part of this document may be disclosed in any manner to a third party without the prior written consent of Philips Product Security and Services Office (PSSO).



100	matrix	401	<input type="checkbox"/>	<input type="checkbox"/>	517	
101	minecraft	401	<input type="checkbox"/>	<input type="checkbox"/>	517	
102	[REDACTED]	200	<input type="checkbox"/>	<input type="checkbox"/>	1600	
<u>Request</u>		<u>Response</u>				
Pretty		Raw				
<pre> 1 POST /viewer/services/user/login.json HTTP/1.1 2 Host: 3.71.200.223 3 Cookie: JSESSIONID=8C58741349EB362E359300C300D51FF 4 Content-Length: 31 5 Sec-Ch-Ua: 6 Content-Type: application/x-www-form-urlencoded 7 X-Requested-With: XMLHttpRequest 8 Sec-Ch-Ua-Mobile: ?0 9 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/114.0.5735.91 Safari/537.36 10 Sec-Ch-Ua-Platform: "" 11 Accept: /* 12 Origin: https://3.71.200.223 13 Sec-Fetch-Site: same-origin 14 Sec-Fetch-Mode: cors 15 Sec-Fetch-Dest: empty 16 Referer: https://3.71.200.223/viewer/patient/query.html 17 Accept-Encoding: gzip, deflate 18 Accept-Language: en-US,en;q=0.9 19 Connection: close 20 21 j_username=root&amp;j_password=[REDACTED] </pre>						

### Old POC:

- Login with username and password multiple times then you will be able to see that the account does not get locked out.

Request ▾	Payload	Status	Error	Timeout	Length	Comment
59	w	401	<input type="checkbox"/>	<input type="checkbox"/>	517	
60	x	401	<input type="checkbox"/>	<input type="checkbox"/>	517	
61	y	401	<input type="checkbox"/>	<input type="checkbox"/>	517	
62	z	401	<input type="checkbox"/>	<input type="checkbox"/>	517	
63	[REDACTED]	200	<input type="checkbox"/>	<input type="checkbox"/>	1600	
<u>Request</u>		<u>Response</u>				
Pretty		Raw				
<pre> 1 POST /admin/services/user/login.json HTTP/1.1 2 Host: ec2-3-70-166-239.eu-central-1.compute.amazonaws.com 3 Cookie: JSESSIONID=582E698AB99CF9F33E7D2610D97C6192 4 Content-Length: 31 5 Sec-Ch-Ua: "Chromium";v="109", "Not_A_Brand";v="99" 6 Content-Type: application/x-www-form-urlencoded 7 X-Requested-With: XMLHttpRequest 8 Sec-Ch-Ua-Mobile: ?0 9 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) 10 Sec-Ch-Ua-Platform: "Windows" 11 Accept: /* 12 Origin: https://ec2-3-70-166-239.eu-central-1.compute.amazonaws.com 13 Sec-Fetch-Site: same-origin 14 Sec-Fetch-Mode: cors 15 Sec-Fetch-Dest: empty 16 Referer: https://ec2-3-70-166-239.eu-central-1.compute.amazonaws.com/admin/login.html 17 Accept-Encoding: gzip, deflate 18 Accept-Language: en-US,en;q=0.9 19 Connection: close 20 21 j_username=root&amp;j_password=[REDACTED] </pre>						

PHILIPS SCOE



Confidential

This document is proprietary and confidential. No part of this document may be disclosed in any manner to a third party without the prior written consent of Philips Product Security and Services Office (PSSO).



Printed copies are uncontrolled unless authenticated.



## 8.10 Webapp: Reflected Cross-Site Scripting (XSS)

Vulnerability Category	Reflected Cross-Site Scripting (XSS)
Vulnerability Category	A3- Injection
Severity	Low
CVSS V3 Calculation	CVSS Base Score: 3.5 CVSS:3.0/AV:N/AC:L/PR:H/UI:R/S:U/C:L/I:L/A:N
Description	<p><b>Vulnerability Description:</b> A Reflected Cross-Site Scripting (XSS) vulnerability occurs when a web application sends strings that are provided by an attacker to a victim's browser in such a way that the browser executes part of the string as code. The string contains malicious data and is passed to the application through a parameter that an attacker can control (For example, a URL parameter or an HTML form field). The application immediately inserts it into its response. This results in the victim's browser executing the attacker's code within a legitimate user's session. Attackers typically exploit reflected XSS vulnerabilities by sending users malicious links containing JavaScript code (For example, via e-mail) or by posting malicious code to other sites that the vulnerable application's users may visit.</p> <p><b>Retest (06-Jun-2023):</b> It is identified that the issue persists.</p> <p><b>Retest (31-Jan-2023):</b> It is identified that self-XSS is still possible &amp; exploitable in multiple places.</p> <p><b>Exploitability rational:</b> Reflected Cross-Site Scripting vulnerabilities give the attacker control of the user's browser. The attack can alter page content with malicious HTML or JavaScript code. The attacker can arbitrarily alter page content displayed to the victim and can execute application functions using the victim's application identity if the victim is authenticated to the application. An often cited example use of a Reflected Cross-Site is where the attacker send themselves to the victim's session identifier. With this session identifier, the attacker can then perform application functions using that user's identity for the duration of that session.</p>

PHILIPS SCOE



Confidential

This document is proprietary and confidential. No part of this document may be disclosed in any manner to a third party without the prior written consent of Philips Product Security and Services Office (PSSO).



	<p><b>Impact rational:</b> Attackers can steal cookies and change the temp look and feel using reflected cross site scripting.</p>
Affected Systems/IP Address/URL	<p>Retest (06-Jun-2023) :</p> <p><a href="https://server_url/viewer/patient/query.html#/0/document/view:medicalDocuments!patentId=&lt;patientID&gt;&lt;PatentAuthID&gt;ISO&amp;documentUniqueIDs=&lt;documentID&gt;">https://server_url/viewer/patient/query.html#/0/document/view:medicalDocuments!patentId=&lt;patientID&gt;&lt;PatentAuthID&gt;ISO&amp;documentUniqueIDs=&lt;documentID&gt;</a></p> <p>Old:</p> <p><a href="https://ec2-3-70-166-239.eu-central-1.compute.amazonaws.com/viewer/services/connect/proxy/flow/sendOruWithPdf">https://ec2-3-70-166-239.eu-central-1.compute.amazonaws.com/viewer/services/connect/proxy/flow/sendOruWithPdf</a></p>
Recommendation	<p>Reflected Cross-Site Scripting (XSS) is prevented by encoding data before inserting it into the generated web page. Each character of the data is encoded and the result string is then inserted onto the generated web page. This technique of encoding values before inserting them on the web page is called "Output Encoding". Output encoding libraries exist for most popular programming languages and frameworks.</p> <p>A web page has seven different output contexts and each output context requires a different encoding scheme. Encode the data using the proper scheme. The seven different encoding schemes are:</p> <ul style="list-style-type: none"> <li>• HTML Text Element</li> <li>• HTML Attribute</li> <li>• URL Parameter</li> <li>• JavaScript Literal</li> <li>• HTML Comment</li> <li>• HTTP Header</li> <li>• CSS Property</li> </ul> <p>For example, the characters: &lt;, &gt;, ", ' are encoded as &amp;#60;, &amp;#62;, &amp;#34;, &amp;#39; for when those characters are inserted into an HTML Text Element. When those characters are inserted as a URL Parameter, the same characters are encoded as %3C, %3E, %22, %27.</p>



	<p>Libraries for implementing the encoding schemes exist for most popular programming languages.</p> <ul style="list-style-type: none"><li>• OWASP Java Encoder: Java only</li><li>• Microsoft Web Protection Library: .NET languages</li><li>• Ruby – escapeHTML() - only supports HTML Text Encoding</li><li>• Jencoder in JQuery: for preventing DOM-based XSS</li></ul> <p>Green field projects can consider the use of other technologies:</p> <ul style="list-style-type: none"><li>• Google Capabilities based JavaScript CAJA</li><li>• OWASP JXT– automatically encodes string data with the proper encoding.</li></ul> <p>Input validation is often recommended as a way to mitigate reflected cross-site scripting. It is insufficient, however, because input validation is used to prevent cross-site scripting only when the data has a strict syntactic format, such as numeric values and dates. Any application inputs which must accept arbitrary data would remain vulnerable.</p>
<b>Status</b>	<b>OPEN</b>

**Steps to Reproduce:****Retest (06-Jun-2023):**

Steps are same as mentioned in 'Retest Status( as on 30 Jan 2023)'.



The screenshot shows a web browser window for the HealthSuite Interoperability Viewer. The URL is <https://3.71.200.223/viewer/patient/query.html#/0/document/viewMedicalDocuments?patientId=2503104&SE%5E%5E%261.3.6.1.4.1.21367.2005.3.7%26ISO&documentUniqueId=d2a3463e-b491-471e-8758-5d3f3c423c0>. The page displays a patient record for Pet, Peter (ID: 2503104 (HOS), Jan 1, 1922 (101 yr), Male) with address 24 Lily street, SC Flow city. A modal dialog box is overlaid on the page, containing the text "An embedded page at 3.71.200.223 says" followed by "xss" and an "OK" button. The entire dialog box is highlighted with a red rectangle.

### Old POC:

Login to Viewer > Patient search >> select any patient >>> medical documents >>>> Add document >>>>> Discharge Note(Ldap lookup) >>>>> fill the form as shown in the below snapshot and then submit, the application server responds with same malicious script without validation or encoding and execute at browser.

The screenshot shows a web browser window for the HealthSuite Interoperability Viewer. The URL is <https://35.176.185.168/viewer/patient/query.html#/0/document/providerMedicalDocuments?patientId=111%5E%5E%5E%262.16.840.1.113883.2.1.4.1%26ISO>. The page displays a patient record for sree<img src="" onerror=alert(1)>, sree<img src="" onerror=alert(2)>. A modal dialog box is overlaid on the page, containing the text "35.176.185.168 says" followed by "101" and an "OK" button. The entire dialog box is highlighted with a red rectangle. Below the dialog, a message box says "Something went wrong". The "Discharge note (LDAP lookup)" tab is selected in the navigation bar.

PHILIPS SCOE



Confidential

This document is proprietary and confidential. No part of this document may be disclosed in any manner to a third party without the prior written consent of Philips Product Security and Services Office (PSSO).



Printed copies are uncontrolled unless authenticated.



Login to Viewer > Patient search >> select any patient >>> medical documents >>> select any xml document >>>> actions >>>>> edit

Parameters: Source Patient ID & Source patient Info

The screenshot shows a list of 5 documents. The 'Edit' action for the second document is highlighted with a red box. The document details are as follows:

Creation date	Title	Author	Author's role	Author's institution	Type
13 Jul 2020 17:01:58	test	makker@ca href="#" onmouseover="alert(2);>sree&ltimg src="" onerror=alert(3)>		Hospital A&ltimg src=x onerror=alert(1)>	Radiology Report
13 Jul 2020 17:01:58	test	makker@ca href="#" onmouseover="alert(2);>sree&ltimg src="" onerror=alert(3)>		Hospital A&ltimg src=x onerror=alert(1)>	Radiology Report
13 Jul 2020 17:01:45	test	makker@ca href="#" onmouseover="alert(2);>sree&ltimg src="" onerror=alert(100)>		Hospital A&ltimg src=x onerror=alert(1)>	Radiology Report
13 Jul 2020 16:57:50	sree&ltimg src="" onerror=alert(100)>	makker@ca href="#" onmouseover="alert(2);>sree&ltimg src="" onerror=alert(100)>		Hospital A&ltimg src=x onerror=alert(1)>	Radiology Report
13 Jul 2020 16:53:14	sree&ltimg src="" onerror=alert(100)>	makker@ca href="#" onmouseover="alert(2);>sree&ltimg src="" onerror=alert(100)>		Hospital A&ltimg src=x onerror=alert(1)>	Radiology Report

The screenshot shows the 'Edit document' page. The 'Source Patient Id' field contains the following malicious XML code:

```
<script><img src="" onerror=alert(2);>sree&ltimg src="" onerror=alert(3)></script>
```

A modal window titled "Something went wrong" is displayed, containing the message "35.176.185.168 says TOO".

### Retest Status( as on 30 Jan 2023)

Issue still persists.

Uploading a pdf which has malicious script.

PHILIPS SCOE



Confidential

This document is proprietary and confidential. No part of this document may be disclosed in any manner to a third party without the prior written consent of Philips Product Security and Services Office (PSSO).



Printed copies are uncontrolled unless authenticated.



This form is supplied as an example that must be configured prior to using it

Document Details

Document: Choose File: Malware\_OWASP Top 10 - 2017.pdf

MIME type

Title

Comments

Document class:

Type: CT Abdomen Report

Author

Author institution: Hospital A

- Upload the file and navigate to Medical Documents section.
- Click the pdf icon for the patient where the document is upload.

Filter results: 3 Documents | Change purpose of use

Creation Date

From: Jan 31, 2023, 6:08:00 PM

Title: CT Abdomen Report

Author: Unknown

Type: CT Abdomen Report

- Scroll the launched pdf and you can see the javascript getting executed.

...c2-3-70-166-239.eu-central-1.compute.amazonaws.com says

OK

Actions View

OWASP Top 10 - 2017

1

TOC Table of Contents

PHILIPS SCOE



Confidential

This document is proprietary and confidential. No part of this document may be disclosed in any manner to a third party without the prior written consent of Philips Product Security and Services Office (PSSO).



Printed copies are uncontrolled unless authenticated.



## 8.11 Webapp: Weak SSL/TLS Configuration

Vulnerability Title	Weak SSL/TLS Configuration
Vulnerability Category	A2 Cryptographic Failures
Severity	Low
CVSS V3 Calculation	CVSS Base Score: 3.1 CVSS:3.1/AV:N/AC:H/PR:L/UI:N/S:U/C:L/I:N/A:N
Description	<p><b>Vulnerability Description:</b> It is observed that the server-side SSL/TLS endpoint is configured to allow weak SSL/TLS cipher suites in the provided server.</p> <p>TLS_RSA_WITH_3DES_EDE_CBC_SHA (rsa 2048)  TLS_ECDHE_RSA_WITH_3DES_EDE_CBC_SHA (rsa 2048)</p> <p><b>Retest (06-Jun-2023):</b> It is identified that the issue persists.</p> <p><b>Exploitability Rational:</b> Some misconfiguration in the server can be used to force the use of a weak cipher - or at worst no encryption - permitting to an attacker to gain access to the supposed secure communication channel. Other misconfiguration can be used for a Denial of Service attack.</p> <p><b>Impact Rational:</b> A server-side SSL/TLS endpoint that supports weak ciphers can allow an attacker to read or modify traffic sent in SSL/TLS connections with that endpoint.</p>
Affected Systems/IP Address/URL	<p>Retest (09/06/2023):</p> <p><a href="https://server_url/">https://server_url/</a></p> <p>Old:</p> <p><a href="https://ec2-3-70-166-239.eu-central-1.compute.amazonaws.com">https://ec2-3-70-166-239.eu-central-1.compute.amazonaws.com</a></p>
Recommendation	Update the server-side TLS endpoint's configuration to allow only TLSv1.2 or TLSv1.3 connections with cipher suites that use the following:

PHILIPS SCOE



Confidential

This document is proprietary and confidential. No part of this document may be disclosed in any manner to a third party without the prior written consent of Philips Product Security and Services Office (PSSO).



Printed copies are uncontrolled unless authenticated.



	<ul style="list-style-type: none"> <li>• Ephemeral Diffie-Hellman for key exchange (Optionally, allow RSA for key exchange if necessary for supporting some clients).</li> <li>• Block ciphers in GCM mode. Note: If CBC mode must be allowed for supporting some clients, use only CBC mode cipher suites that use the SHA2 family of hash functions (SHA256, SHA384, SHA512).</li> </ul>
Status	Open

## Steps to Reproduce

**Retest (06-Jun-2023):**

Steps are same as before.

```

xds_443_ssl_enum x
1 # Nmap 7.93 scan initiated Mon May 29 14:13:19 2023 as: nmap -p 443 --script=ssl* -oN nmap/xds_443_ssl_enum -v -d [18.196.27.233]
2 --Timing report -----
3 hostgroups: min 1, max 10000
4 rtt-timeouts: init 1000, min 100, max 10000
5 max-scan-delay: TCP 1000, UDP 1000, SCTP 1000
6 parallelism: min 0, max 0
7 max-retries: 10, host-timeout: 0
8 min-rate: 0, max-rate: 0
9 -----
10 Nmap scan report for [ec2-18-196-27-233.eu-central-1.compute.amazonaws.com (18.196.27.233)]
11 Host is up, received syn-ack (0.16s latency).
12 Scanned at 2023-05-29 14:13:20 IST for 12s
13
14 PORT      STATE SERVICE REASON
15 443/tcp    open  https   syn-ack
16 | ssl-enum-ciphers:
17 |   TLSv1.2:
18 |     ciphers:
19 |       TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 (ecdh_x25519) - A
20 |       TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 (ecdh_x25519) - A
21 |       TLS_ECDHE_RSA_WITH_CHACHA20_POLY1305_SHA256 (ecdh_x25519) - A
22 |       TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA (ecdh_x25519) - A
23 |       TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA (ecdh_x25519) - A
24 |       TLS_RSA_WITH_AES_128_GCM_SHA256 (rsa_2048) - A
25 |       TLS_RSA_WITH_AES_256_GCM_SHA384 (rsa_2048) - A
26 |       TLS_RSA_WITH_AES_128_CBC_SHA (rsa_2048) - A
27 |       TLS_RSA_WITH_AES_256_CBC_SHA (rsa_2048) - A
28 |       TLS_ECDHE_RSA_WITH_3DES_EDE_CBC_SHA (ecdh_x25519) - C
29 |       TLS_RSA_WITH_3DES_EDE_CBC_SHA (rsa_2048) - C
30 | compressors:
31 |   NULL
32 | cipher preference: server
33 | warnings:
34 |   64-bit block cipher 3DES vulnerable to SWEET32 attack

```

## Old POC:

Use nmap to enumerate the ciphers used by the application end-points.

PHILIPS SCOE



Confidential

This document is proprietary and confidential. No part of this document may be disclosed in any manner to a third party without the prior written consent of Philips Product Security and Services Office (PSSO).



Printed copies are uncontrolled unless authenticated.



Starting Nmap 7.92 ( https://nmap.org ) at 2023-01-23 18:30 India Standard Time  
 Nmap scan report for ec2-3-70-166-239.eu-central-1.compute.amazonaws.com (3.70.166.239)  
 Host is up (0.14s latency).

```

PORT      STATE SERVICE
443/tcp    open  https
|_ssl-enum-ciphers:
  TLSv1.2:
    ciphers:
      TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 (ecdh_x25519) - A
      TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 (ecdh_x25519) - A
      TLS_ECDHE_RSA_WITH_CHACHA20_POLY1305_SHA256 (ecdh_x25519) - A
      TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA (ecdh_x25519) - A
      TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA (ecdh_x25519) - A
      TLS_RSA_WITH_AES_128_GCM_SHA256 (rsa_2048) - A
      TLS_RSA_WITH_AES_256_GCM_SHA384 (rsa_2048) - A
      TLS_RSA_WITH_AES_128_CBC_SHA (rsa_2048) - A
      TLS_RSA_WITH_AES_256_CBC_SHA (rsa_2048) - A
      TLS_ECDHE_RSA_WITH_3DES_EDE_CBC_SHA (ecdh_x25519) - C
      TLS_RSA_WITH_3DES_EDE_CBC_SHA (rsa_2048) - C
    compressors:
      NULL
    cipher preference: server
    warnings:
      64-bit block cipher 3DES vulnerable to SWEET32 attack
  TLSv1.3:
    ciphers:
      TLS_AKE_WITH_AES_128_GCM_SHA256 (ecdh_x25519) - A
      TLS_AKE_WITH_CHACHA20_POLY1305_SHA256 (ecdh_x25519) - A
      TLS_AKE_WITH_AES_256_GCM_SHA384 (ecdh_x25519) - A
    cipher preference: server
  |_ least strength: C

Nmap done: 1 IP address (1 host up) scanned in 12.22 seconds

```

## 9. Tools Used

Scope	Tools Used
Application Security	Burpsuite pro, nmap

## 10. Automated Tool Report

NA

PHILIPS SCOE



Confidential

This document is proprietary and confidential. No part of this document may be disclosed in any manner to a third party without the prior written consent of Philips Product Security and Services Office (PSSO).



Printed copies are uncontrolled unless authenticated.



## 11. Manual Test Reports and Test Case Execution



Testsuite\_WebApp.xls

X

PHILIPS SCOE



Confidential

This document is proprietary and confidential. No part of this document may be disclosed in any manner to a third party without the prior written consent of Philips Product Security and Services Office (PSSO).

60

Printed copies are uncontrolled unless authenticated.