

OpenMRS Multiple Vulnerabilities

Medium

[← View More Research Advisories](#)

Synopsis

Tenable Research has discovered a number of security-related issues in the OpenMRS Reference Application. We have confirmed these issues exist in version 2.9.0.

The details of these issues are as follows:

XSS via Referrer Headers and Arbitrary Parameters

The application copies "Referer" header values into an html element named "redirectUrl" within many webpages (such as login.htm). There is insufficient validation for this parameter, which allows for the possibility of cross-site scripting.

The following is an example curl command to illustrate the issue:

```
curl -i -s -k -X 'GET' -H '$Host: 10.0.0.54:8082' -H '$Referer: http://10.0.0.54:8082/openmrs-standalone/'>asdf<script>alert(1);</script>asdf' '$http://10.0.0.54:8082/openmrs-standalone/login.htm'
```

CVSSv2: (AV:N/AC:M/Au:N/C:P/I:P/A:P) - 6.8

XSS in UIFramework Error Page

The UI Framework Error Page reflects arbitrary, user-supplied input back to the browser, which can result in XSS. Any page that is able to trigger a UI Framework Error is susceptible to this issue.

The following is an example of this issue: `http://<host>/<openmrs path>/coreapps%3Cimg%20src=a%20onerror=alert(1)%3E/findpatient/findPatient.page`

The above payload decodes to: ``

This payload can be used in almost any path for the OpenMRS application as far as I can tell.

CVSSv2: (AV:N/AC:M/Au:N/C:P/I:P/A:P) - 6.8

XSS in Login Page's sessionLocation parameter

The sessionLocation parameter for the login page is vulnerable to cross-site scripting. Using the following payload for the parameter illustrates the issue: `<script>alert(1);</script>`

CVSSv2: (AV:N/AC:M/Au:N/C:P/I:P/A:P) - 6.8

XSS in ActiveVisit page's app parameter

The app parameter for the ActiveVisit's page is vulnerable to cross-site scripting.

For example: `http://<host>/<openmrs path>/coreapps/activeVisits.page?app=coreapps.activeVisits"><script>alert(1)</script>`

This attack requires authentication.

CVSSv2: (AV:N/AC:M/Au:S/C:P/I:P/A:P) 6.0

Authentication Bypass for Data Import

The import functionality of the Data Exchange Module does not properly redirect to a login page when an unauthenticated user attempts to access it. For example, by visiting "http://<host>/<openmrs path>/module/dataexchange/import.form" directly, any user is able to import arbitrary information.

CVSSv2: (AV:N/AC:L/Au:N/C:N/I:P/A:P) - 6.4

Authentication Bypass for Data Export

The export functionality of the Data Exchange Module does not properly redirect to a login page when an unauthenticated user attempts to access it. For example, by visiting "http://<host>/<openmrs path>/module/dataexchange/export.form" directly, any user is able to export potentially sensitive information.

CVSSv2: (AV:N/AC:L/Au:N/C:P/I:I/N/A:N) - 5.0

Solution



January 6, 2020 - Tenable attempts to establish security contact.

January 6, 2020 - Tenable discloses to security@openmrs.org. April 5, 2020 marks 90 days.

January 7, 2020 - OpenMRS acknowledges report, but has an email malfunction. They request disclosure to be resent.

January 7, 2020 - Tenable resends disclosure.

January 20, 2020 - OpenMRS claims they did not receive clarification message.

January 21, 2020 - Tenable resends disclosure.

January 21, 2020 - OpenMRS acknowledges disclosure and requests extension.

January 22, 2020 - Tenable denies request, but states it can be revisited later in the process.

January 27, 2020 - OpenMRS provides drafted patches and patched standalone version for testing.

January 28, 2020 - Tenable acknowledges.

March 2, 2020 - Tenable requests status update.

April 1, 2020 - OpenMRS states that fixes should be deployed by end of week (April 3).

April 2, 2020 - Tenable acknowledges.

April 5, 2020 - OpenMRS states that fixes are out.

All information within TRA advisories is provided "as is", without warranty of any kind, including the implied warranties of merchantability and fitness for a particular purpose, and with no guarantee of completeness, accuracy, or timeliness. Individuals and organizations are responsible for assessing the impact of any actual or potential security vulnerability.

Tenable takes product security very seriously. If you believe you have found a vulnerability in one of our products, we ask that you please work with us to quickly resolve it in order to protect customers. Tenable believes in responding quickly to such reports, maintaining communication with researchers, and providing a solution in short order.

For more details on submitting vulnerability information, please see our [Vulnerability Reporting Guidelines](#) page.

If you have questions or corrections about this advisory, please email advisories@tenable.com

Risk Information

CVE ID: [CVE-2020-5728](#)

[CVE-2020-5729](#)

[CVE-2020-5730](#)

[CVE-2020-5731](#)

[CVE-2020-5732](#)

[CVE-2020-5733](#)

Tenable Advisory ID: TRA-2020-18

Credit: Jimi Sebree

CVSSv2 Base / Temporal Score: 6.8 / 5.6

CVSSv2 Vector: (AV:N/AC:M/Au:N/C:P/I:P/A:P)

Affected Products: OpenMRS 2.9.0 and prior

Risk Factor: Medium

Advisory Timeline

April 6, 2020 - Initial release

FEATURED PRODUCTS

Tenable One Exposure Management Platform

Tenable.cs Cloud Security

Tenable.io Vulnerability Management

Tenable.io Web App Scanning

Tenable.asm External Attack Surface

Tenable.ad Active Directory

Tenable.ot Operational Technology

Tenable.sc Security Center

Tenable Lumin

Nessus

→ View all Products

FEATURED SOLUTIONS

Application Security

Building Management Systems

Cloud Security Posture Management

Compliance

Exposure Management

Finance

Healthcare

IT/OT



Vulnerability Management

Zero Trust

→ View all Solutions

CUSTOMER RESOURCES

Resource Library

Community & Support

Customer Education

Tenable Research

Documentation

Trust and Assurance

Nessus Resource Center

Cyber Exposure Fundamentals

System Status

CONNECTIONS

Blog

Contact Us

Careers

Investors

Events

Media



[Privacy Policy](#) [Legal](#) [508 Compliance](#)

© 2022 Tenable®, Inc. All Rights Reserved

