Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal') in OpenClinica

Moderate **svadla-oc** published **GHSA-9rrv-prff-qph7** on May 11

Package

OpenClinica (None)

Affected versions	Patched versions
<3.16	3.13.1, 3.14.1, 3.16.2

Description

Impact

The following vulnerabilities were identified by CodeQL and can be found here:

- https://lgtm.com/projects/g/OpenClinica/OpenClinica/alerts/?mode=list&tag=security&id=java%2Fpath-injection

A summary of the above can be found below.

The following endpoints contain path traversal vulnerabilities.

Arbitrary File Read Vulnerabilities

They allow an attacker to arbitrarily download any file from a system running OpenClinica. This allows an attacker to steal any information/files stored on a system running OpenClinica.

The following endpoints are impacted:

- `/forms/migrate/{filename}/downloadLogFile`
  - Source:

OpenClinica/web/src/main/java/org/akaza/openclinica/controller/BatchCRFMigrationController.java
Line 129 in e46944f

```
129     File fileToDownload = new File(logFileName);
```

- `/DownloadVersionSpreadSheet` via the `fileName` form post parameter
  - For users with the permissions: 'system admin', `STUDYDIRECTOR` , or `COORDINATOR`
  - Source:

OpenClinica/web/src/main/java/org/akaza/openclinica/control/admin/DownloadVersionSpreadSheetServlet.java
Lines 93 to 95 in `e46944f`

```
93      excelFile = new File(dir + excelFileName);
94      // backwards compat
95      File oldExcelFile = new File(dir + oldExcelFileName);
```

Arbitrary File Write Vulnerabilities

The following allow an attacker to upload any file they wish to any directory they wish on a system running OpenClinica. This can lead to remote code execution in certain environments.

- `/openrosa/{studyOID}/submission` by modifying the `studyOID` with a path traversal payload.
  - Source:

OpenClinica/web/src/main/java/org/akaza/openclinica/controller/openrosa/OpenRosaSubmissionController.java
Line 108 in `e46944f`

```
108     if (!new File(dir).exists()) new File(dir).mkdirs();
```

Patches

`6f864e8`

Workarounds

Is there a way for users to fix or remediate the vulnerability without upgrading?
No

References

- https://owasp.org/www-community/attacks/Path_Traversal

Severity

Moderate 6.5 / 10

CVSS base metrics

Attack vector	Network
Attack complexity	Low
Privileges required	Low
User interaction	None

Scope	**Unchanged**
Confidentiality	**High**
Integrity	**None**
Availability	**None**

CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N

CVE ID

CVE-2022-24830

Weaknesses

CWE-22

Credits

JLLeitschuh