Directory Traversal in OpenMRS Startup Filter

High gracepotma published GHSA-8rgr-ww69-jv65 on Feb 22

Package

openmrs (N/A)

Affected versions

>= 1.6

Patched versions

2.1.5, 2.2.1, 2.3.5, 2.4.5, 2.5.3

Description

Impact

Arbitrary file exfiltration due to failure to sanitize request when satisfying GET requests for `/images` & `/initfilter/scripts` . This can allow an attacker to access any file on a system running OpenMRS that is accessible to the user id OpenMRS is running under.

Vulnerability location:

- https://lgtm.com/projects/g/openmrs/openmrs-core/snapshot/fb1335c925ca4c94be5a546707b90d2c1efa4dcc/files/web/src/main/java/org/openmrs/web/filter/StartupFilter.java#L123
- openmrs-core/web/src/main/java/org/openmrs/web/filter/StartupFilter.java
  Line 123 in ee3373a

```
123      file = new File(file, httpRequest.getPathInfo());
```

```
if (servletPath.startsWith("/images") || servletPath.startsWith("/initfi
        servletPath = servletPath.replaceFirst("/initfilter", "/WEB-INF/
        // writes the actual image file path to the response
        File file = new File(filterConfig.getServletContext().getRealPat
        if (httpRequest.getPathInfo() != null) {
                file = new File(file, httpRequest.getPathInfo()); // VUL
        }

        InputStream imageFileInputStream = null;
```

```
try {
        imageFileInputStream = new FileInputStream(file);
        OpenmrsUtil.copyFile(imageFileInputStream, httpResponse.
}
```

Patches

Affected implementations should update to the latest patch version of OpenMRS Core for the minor version they use. These are:

- 2.1.5
- 2.2.1
- 2.3.5
- 2.4.5
- 2.5.3

Patch that fixes this vulnerability can be found here: `db8454b` #diff-7c64d9f61d4d4e2ddba92920d7cf63ec96091b308d43904956b3846bc0c26d80R128

Workarounds and Mitigation

As a general rule, this vulnerability is already mitigated by Tomcat's URL normalization in Tomcat 7.0.28+. Implementers on older versions of Tomcat should consider upgrading their Tomcat instance as well as their OpenMRS instance.

For more information

If you have any questions or comments about this advisory:

- Email us at security@openmrs.org

Severity

High 7.5 / 10

CVSS base metrics

Attack vector	Network
Attack complexity	Low
Privileges required	None
User interaction	None
Scope	Unchanged
Confidentiality	High

Integrity	**None**
Availability	**None**

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

CVE ID

CVE-2022-23612

Weaknesses

No CWEs

Credits

 **JLLeitschuh**