Symlink Directory Exposes Webapp Directory Contents

Low **waynebeaton** published **GHSA-j6qj-j888-vvgq** on Apr 1, 2021

Package

org.eclipse.jetty:jetty-deploy (Maven)

Affected versions	Patched versions
9.4.32-9.4.38, 10.0.0.beta2-10.0.1, 11.0.0.beta2-11.0.1	9.4.39, 10.0.2, 11.0.2

Description

Impact

If the `${jetty.base}` directory or the `${jetty.base}/webapps` directory is a symlink (soft link in Linux), the contents of the `${jetty.base}/webapps` directory may be deployed as a static web application, exposing the content of the directory for download.

For example, the problem manifests in the following `${jetty.base}` :

```
demo-base/
├── etc
├── lib
├── resources
├── start.d
├── deploy
│   └── async-rest.war
└── webapps -> deploy
```

Workarounds

Do not use a symlink

Severity

Low 2.7 / 10

CVSS base metrics	
Attack vector	Network
Attack complexity	Low
Privileges required	High
User interaction	None
Scope	Unchanged
Confidentiality	Low
Integrity	None
Availability	None

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

CVE ID

CVE-2021-28163

Weaknesses

CWE-200

Credits

svarovski