April 20, 2022

GHSL-2022-008: Path traversal in the OWASP Enterprise Security API (ESAPI)- CVE-2022-23457

Jaroslav Lobacevski

Coordinated Disclosure Timeline

- 2022/01/31: Report sent to maintainers.
- 2022/01/31: Receipt acknowledged.
- 2022/04/17: v2.3.0.0 with a fix was released.

Summary

`getValidDirectoryPath` incorrectly treats sibling of a root directory as a child.

Product

The OWASP Enterprise Security API (ESAPI)

Tested Version

v2.2.3.1 (The latest version of “Legacy” 2.x branch as ESAPI 3.x is in early development and has no releases yet.)

Details

Issue: `getValidDirectoryPath` bypass (`GHSL-2022-008`)

`parent` [1] - the third parameter in `getValidDirectoryPath` is used to validate that the `input` [2] path is “inside specified parent” directory [3].

```
public String getValidDirectoryPath(String context, String input /* [2] */, File parent /* [1] */, boolean allowNull) throws ValidationExcepti
...
  // [3]
        if ( !dir.getCanonicalPath().startsWith(parent.getCanonicalPath() ) ) {
                throw new ValidationException( context + ": Invalid directory name", "Invalid directory, not inside specified parent: context=
        }
...
}
```

If the result of `parent.getCanonicalPath()` is not slash terminated it allows for partial path traversal.

Consider `"/usr/outnot".startsWith("/usr/out")`. The check is bypassed although `outnot` is not under the `out` directory. The terminating slash may be removed in various places. On Linux `println(new File("/var/"))` returns `/var`, but `println(new File("/var", "/"))` - `/var/`, however `println(new File("/var", "/").getCanonicalPath())` - `/var`.

Impact

This issue allows to break out of expected directory.

CVE

- CVE-2022-23457

Credit

This issue was discovered and reported by GHSL team member @JarLob (Jaroslav Lobačevski).

Contact

You can contact the GHSL team at `securitylab@github.com`, please include a reference to `GHSL-2022-008` in any communication regarding this issue.

Product

- Features
- Security
- Enterprise
- Customer stories
- Pricing
- Resources

Platform

- Developer API
- Partners
- Atom
- Electron
- GitHub Desktop

Support

- Docs
- Community Forum
- Professional Services
- Status
- Contact GitHub

Company

- About
- Blog
- Careers
- Press
- Shop

- in

-
- Terms
- Privacy
- Cookie settings