

Esri Third-Party OSS/FOSS

Software Acknowledgements

*This document acknowledges certain third parties whose software may be used in Esri products. The most recent version of this document can be found at* <http://www.esri.com/legal/open-source-acknowledgements>.

*While Esri makes every effort to ensure that citations in this document are complete and accurate, errors may occur. If you see an error or omission, please help us improve this disclosure document by sending information to* [oss@esri.com](mailto:oss@esri.com).

*Some Open-Source licenses require that the original or modified source code of an included project be made available. To request source code for any project covered under such license terms, send a request identifying the specific project to* [oss@esri.com](mailto:oss@esri.com).

Disclosed components will be found in the accompanying ArcGIS Maps SDK 2.2.0 for Game Engines Open-Source Components spreadsheet for each of the development environments. Each spreadsheet contains information about Open-Source Components and the internal ArcGIS Maps SDK resource that uses the component. For each Open-Source Component specific artifacts are provided in the Component License Artifacts folder -the spreadsheet lists the folder to look in for component artifacts. Additional artifacts will include the component license, and may include other items such as author lists, patent notices, and other dependent component licenses. These folders may contain additional artifacts from components not included in the Maps SDK.

**Note on glew and zlib:**

The Open-Source component “glew” comes up as a false positive with some component scanners. Glew is not used with the ArcGIS Maps SDKs.

The Open-Source component “zlib” comes up as a false positive with some component scanners. Zlib has been replaced with zlib-ng.

**Resolved Vulnerabilities, not exposed:**

Assimp version 6.0.2

* [CVE-2025-11277](https://nvd.nist.gov/vuln/detail/CVE-2025-11277)

Triage Info:

The vulnerability is with the Q3D data format which is disabled using the ASSIMP\_BUILD\_NO\_Q3D\_IMPORTER define

* [CVE-2025-11274](https://nvd.nist.gov/vuln/detail/CVE-2025-11274)

Triage Info:

The vulnerability is with the Q3D data format which is disabled using the ASSIMP\_BUILD\_NO\_Q3D\_IMPORTER define

* [CVE-2025-11275](https://nvd.nist.gov/vuln/detail/CVE-2025-11275)

Triage Info:

And OpenDDLParser.h is included only in OpenGEXImporter.cpp and this spec is disabled in our builds.

json-c version 0.15.0

* [CVE-2020-12762](https://nvd.nist.gov/vuln/detail/CVE-2020-12762)  
  Triage Info:  
  json-c 0.15 contains the fix referenced by the CVE.
* [CVE-2021-32292](https://nvd.nist.gov/vuln/detail/CVE-2021-32292)   
  Triage Info:  
  This CVE is in the command line tool and is not included in the Native SDKs

Libpng 1.6.39

* [CVE-2025-64720](https://nvd.nist.gov/vuln/detail/CVE-2025-64720)  
  Triage Info:  
  The Native SDKs do not set the PNG\_FLAG\_OPTIMIZE\_ALPHA which is necessary for to exploit this vulnerability.
* [CVE-2025-64505](https://nvd.nist.gov/vuln/detail/CVE-2025-64505)   
  Triage Info:  
  The Native SDKs do not define PNG\_READ\_QUANTIZE\_SUPPORTED which is necessary to enable this function.
* [CVE-2025-64506](https://nvd.nist.gov/vuln/detail/CVE-2025-64506)  
  Triage Info:  
  The Native SDKs do not make use of this function.
* [CVE-2025-65018](https://nvd.nist.gov/vuln/detail/CVE-2025-65018)  
  Triage Info:  
  The Native SDKs do not decode PNGs this way.

Giflib 5.1.9

* [CVE-2025-31344](https://nvd.nist.gov/vuln/detail/CVE-2025-31344)  
  Triage Info:  
  The giflib problem function is LoadRGB and the only place that is referenced is in the RGB2GIF function in giflib itself. The Native SDKs do not use giflib directly. GDAL uses Giflib but doesn't reference either of those functions.

**Acknowledged Vulnerabilities in ArcGIS Maps SDK 2.2.0 at the time of release:**

Libpng 1.6.39

* [CVE-2025-66293](https://nvd.nist.gov/vuln/detail/CVE-2025-66293)

Triage Info:

This is a known vulnerability to the Native SDKs.

Expat version 2.7.3

* [CVE-2025-66382](https://nvd.nist.gov/vuln/detail/CVE-2025-66382)

Triage Info:

This is a known vulnerability in the Native SDKs.