# Legal Disclaimer

Copyright and all other rights reserved by Reliable Energy Analytics, LLC (REA) 2018-2021.

Others are free to use this “boilerplate” template under the Creative Commons V4.0 license terms.

DISCLAIMER OF WARRANTIES

TO THE EXTENT NOT PROHIBITED BY LAW, REA HEREBY DISCLAIMS ALL EXPRESS OR IMPLIED REPRESENTATIONS, WARRANTIES, GUARANTEES, AND CONDITIONS OF ANY KIND, ARISING BY LAW OR OTHERWISE, WITH REGARD TO THIS ARTIFACT, INCLUDING BUT NOT LIMITED TO REPRESENTATIONS, WARRANTIES, GUARANTEES, AND CONDITIONS OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, TITLE, NONINFRINGEMENT, AND QUALITY OF SERVICE.

REA MAKES NO REPRESENTATIONS OR WARRANTIES REGARDING THE CONTENT, EFFECTIVENESS, USEFULNESS, RELIABILITY, AVAILABILITY, TIMELINESS, QUALITY, SUITABILITY, ACCURACY OR COMPLETENESS OF THIS ARTIFACT OR THE RESULTS YOU MAY OBTAIN BY USING THE ARTIFACT OR THAT THE ARTIFACT WILL BE ERROR-FREE.

# Known Vulnerabilities Disclosure

Last Modified Date: 2021-10-23

Boilerplate Version: 1.0.1

An XML Schema and example Vulnerability Report in XML is available online at: <https://github.com/rjb4standards/REA-Products>

Fix Status MUST be one of the following values:

* N/A
* Fix Available
* Not Fixed
* No Plans to Fix
* Pending Development
* In Development
* In Test
* Planned Fix this Year
* Planned Future Fix
* Investigating
* Confirmed Issue
* Unknown

Refer to the appropriate Product entry contained in the Vendor Response XML File, SBOM URL element for information on the list of components referred to in this disclosure, e.g.

<SAG:SBOM type="cycloneDX" version="1.2" format="XML" signature="https://softwareassuranceguardian.com/REDACTED">**https://softwareassuranceguardian.com/REDACTED**</SAG:SBOM>

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **Product** | **Version** | **Component/Version** | **Supplier** | **CVE ID** | **Fix Status** | **REA Analysis and Findings** |
| SAG-PM | 1.1.4 | cryptography/3.3.1 | The cryptography developers | [CVE-2020-36242](https://services.nvd.nist.gov/rest/json/cves/1.0?keyword=cryptography+3.3.1) | N/A | This vulnerability is exploited during file encryption. SAG-PM does not perform file encryption using this component and is most likely not vulnerable to this CVE |
| SAG-PM | 1.1.4 | cryptography/3.3.1 | The cryptography developers | [CVE-2014-8564](https://services.nvd.nist.gov/rest/json/cves/1.0?keyword=cryptography+3.3.1) | N/A | This vulnerability is exploited when Elliptic curve certificates are used. SAG-PM does not perform any elliptic curve certificate functions from this component and is most likely not vulnerable to this CVE |
| SAG-PM | 1.1.4 | idna/2.10 | Kim Davies | [CVE-2012-4870](https://services.nvd.nist.gov/rest/json/cves/1.0?keyword=idna+2.10) | N/A | This is a false positive from NIST NVD. The actual component listed in the CVE is not used in SAG-PM. |
| SAG-PM | 1.1.4 | idna/2.10 | Kim Davies | [CVE-2006-4346](https://services.nvd.nist.gov/rest/json/cves/1.0?keyword=idna+2.10) | N/A | This is a false positive from NIST NVD. The actual component listed in the CVE is not used in SAG-PM. |
| SAG-PM | 1.1.4 | ply/3.11 | David Beazley | [CVE-2020-12100](https://services.nvd.nist.gov/rest/json/cves/1.0?keyword=ply+3.11) | N/A | This is a false positive from NIST NVD. The actual component listed in the CVE is not used in SAG-PM. |
| SAG-PM | 1.1.4 | ply/3.11 | David Beazley | [CVE-2019-18183](https://services.nvd.nist.gov/rest/json/cves/1.0?keyword=ply+3.11) | N/A | This is a false positive from NIST NVD. The actual component listed in the CVE is not used in SAG-PM. |
| SAG-PM | 1.1.4 | ply/3.11 | David Beazley | [CVE-2011-1487](https://services.nvd.nist.gov/rest/json/cves/1.0?keyword=ply+3.11) | N/A | This is a false positive from NIST NVD. The actual component listed in the CVE is not used in SAG-PM. |