



# CVE-2021-21238

[MITRE](#)[NVD](#)[CVE.ORG](#)[JSON API](#)[Print: PDF](#)

## Summary

|                        |                                                                                                                      |
|------------------------|----------------------------------------------------------------------------------------------------------------------|
| <b>CVE</b>             | CVE-2021-21238                                                                                                       |
| <b>State</b>           | PUBLIC                                                                                                               |
| <b>Assigner</b>        | security-advisories@github.com                                                                                       |
| <b>Source Priority</b> | CVE Program / NVD first with legacy fallback                                                                         |
| <b>Published</b>       | 2021-01-21 15:15:00 UTC                                                                                              |
| <b>Updated</b>         | 2021-01-29 17:58:00 UTC                                                                                              |
| <b>Description</b>     | PySAML2 is a pure python implementation of SAML Version 2 Standard. PySAML2 before 6.5.0 has an improper verificatio |

## Risk And Classification

**Problem Types:** CWE-347

## NVD Known Affected Configurations (CPE 2.3)

| Type        | Vendor                          | Product                 | Version | Update | Edition | Language |
|-------------|---------------------------------|-------------------------|---------|--------|---------|----------|
| Application | <a href="#">Pysaml2 Project</a> | <a href="#">Pysaml2</a> | All     | All    | All     | All      |
| Application | <a href="#">Pysaml2 Project</a> | <a href="#">Pysaml2</a> | All     | All    | All     | All      |

## References

| Reference                                                                                             | Source  | Link                         | Tags                 |
|-------------------------------------------------------------------------------------------------------|---------|------------------------------|----------------------|
| <a href="#">pysaml2 · PyPI</a>                                                                        | MISC    | <a href="#">pypi.org</a>     | Product, Third Party |
| <a href="#">Processing of invalid SAML XML documents · Advisory · IdentityPython/pysaml2 · GitHub</a> | CONFIRM | <a href="#">github.com</a>   | Third Party Adviso   |
| <a href="#">Merge pull request from GHSA-f4g9-h89h-jgv9 · IdentityPython/pysaml2@1d8fd26 · GitHub</a> | MISC    | <a href="#">github.com</a>   | Patch, Third Party   |
| <a href="#">Release Version 6.5.0 · IdentityPython/pysaml2 · GitHub</a>                               | MISC    | <a href="#">github.com</a>   | Third Party Adviso   |
| <a href="#">CVE Program record</a>                                                                    | CVE.ORG | <a href="#">www.cve.org</a>  | canonical            |
| <a href="#">NVD vulnerability detail</a>                                                              | NVD     | <a href="#">nvd.nist.gov</a> | canonical, analysis  |

No vendor comments have been submitted for this CVE.

## Legacy QID Mappings

[179845](#) Debian Security Update for python-pysaml2 (CVE-2021-21238)

[501905](#) Alpine Linux Security Update for py3-saml2

[690445](#) Free Berkeley Software Distribution (FreeBSD) Security Update for pysaml2 (fb67567a-5d95-11eb-a955-08002728f74c)

[982964](#) Python (pip) Security Update for pysaml2 (GHSA-f4g9-h89h-jgv9)

© [CVE.report](#) 2026 |

Use of this information constitutes acceptance for use in an AS IS condition. There are NO warranties, implied or otherwise, with regard to this information or its use. Any use of this information is at the user's risk. It is the responsibility of user to evaluate the accuracy, completeness or usefulness of any information, opinion, advice or other content. EACH USER WILL BE SOLELY RESPONSIBLE FOR ANY consequences of his or her direct or indirect use of this web site. ALL WARRANTIES OF ANY KIND ARE EXPRESSLY DISCLAIMED. This site will NOT BE LIABLE FOR ANY DIRECT, INDIRECT or any other kind of loss.

CVE, CWE, and OVAL are registered trademarks of [The MITRE Corporation](#) and the authoritative source of CVE content is [MITRE's CVE web site](#). This site includes MITRE data granted under the following [license](#).

**Free CVE JSON API** [cve.report/api](#)

**CVE.report and Source URL Uptime Status** [status.cve.report](#)