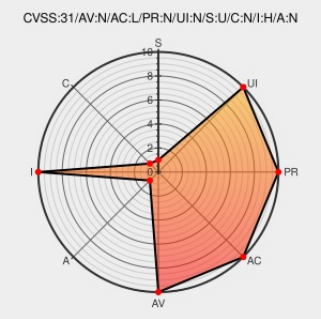
# CVE-2018-5387

Published on: 07/24/2018 12:00:00 AM UTC

Last Modified on: 06/01/2022 08:24:00 PM UTC

## CVE-2018-5387

Source: Mitre | Source: NIST | CVE.ORG | Print: PDF




Certain versions of Samlbase from Wizkunde contain the following vulnerability:

Wizkunde SAMLBase may incorrectly utilize the results of XML DOM traversal and canonicalization APIs in such a way that an attacker may be able to manipulate the SAML data without invalidating the cryptographic signature, allowing the attack to potentially bypass authentication to SAML service providers.

CVE-2018-5387 has been assigned by cert@cert.org to track the vulnerability - currently rated as HIGH severity.

Affected Vendor/Software: **Wizkunde** - **SAMLBase** version **< 1.2.7**

### CVSS3 Score: 7.5 - HIGH

| Attack Vector | Attack Complexity | Privileges Required | User Interaction |
|---|---|---|---|
| NETWORK | LOW | NONE | NONE |
| **Scope** | **Confidentiality Impact** | **Integrity Impact** | **Availability Impact** |
| UNCHANGED | NONE | HIGH | NONE |

### CVSS2 Score: 5 - MEDIUM

| Access Vector | Access Complexity | Authentication |
|---|---|---|
| NETWORK | LOW | NONE |
| **Confidentiality Impact** | **Integrity Impact** | **Availability Impact** |
| NONE | PARTIAL | NONE |

### CVE References

| Description | Tags | Link |
|---|---|---|
| Duo Finds SAML Vulnerabilities | Exploit | MISC duo.com/blog/duo-finds-saml-vulnerabilities-affecting-multiple-imple |

| | | |
|---|---|---|
| Affecting Multiple Implementations \| Duo Security | Third Party Advisory<br>duo.com<br>text/html | |
| VU#475445 - Multiple SAML libraries may allow authentication bypass via incorrect XML canonicalization and DOM traversal | Third Party Advisory<br>US Government Resource<br>www.kb.cert.org<br>text/html | CERT-VN VU#475445 |
| Fixed comment vulnerability in verifying signatures · GoGentoOSS/SAMLBase@482cdf8 · GitHub | github.com<br>text/html | CONFIRM github.com/GoGentoOSS/SAMLBase/commit/482cdf8c090e0f1179073034el |
| SAML Vulnerability · Issue #3 · GoGentoOSS/SAMLBase · GitHub | github.com<br>text/html | CONFIRM github.com/GoGentoOSS/SAMLBase/issues/3 |

By selecting these links, you may be leaving CVEreport webspace. We have provided these links to other websites because they may have information that would be of interest to you. No inferences should be drawn on account of other sites being referenced, or not, from this page. There may be other websites that are more appropriate for your purpose. CVEreport does not necessarily endorse the views expressed, or concur with the facts presented on these sites. Further, CVEreport does not endorse any commercial products that may be mentioned on these sites. Please address comments about any linked pages to comment@cve.report.

There are currently no QIDs associated with this CVE

## Known Affected Configurations (CPE V2.3)

| Type | Vendor | Product | Version | Update | Edition | Language |
|---|---|---|---|---|---|---|
| Application | Wizkunde | Samlbase | All | All | All | All |
| Application | Wizkunde | Samlbase | - | All | All | All |
| Application | Wizkunde | Samlbase | - | All | All | All |

cpe:2.3:a:wizkunde:samlbase:*:*:*:*:*:*:*:*:

cpe:2.3:a:wizkunde:samlbase:-:*:*:*:*:*:*:*:

cpe:2.3:a:wizkunde:samlbase:-:*:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→