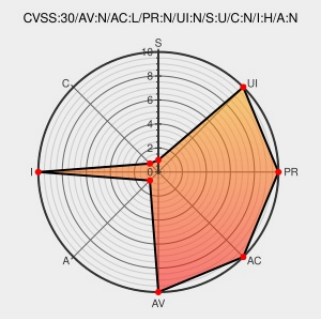
CVE-2018-1000531

Published on: 06/26/2018 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:24:30 PM UTC

CVE-2018-1000531

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



Certain versions of Prime-jwt from Inversoft contain the following vulnerability:

inversoft prime-jwt version prior to commit abb0d479389a2509f939452a6767dc424bb5e6ba contains a CWE-20 vulnerability in JWTDecoder.decode that can result in an incorrect signature validation of a JWT token. This attack can be exploitable when an attacker crafts a JWT token with a valid header using 'none' as algorithm and a body to requests it be validated. This vulnerability was fixed after commit abb0d479389a2509f939452a6767dc424bb5e6ba.

CVE-2018-1000531 has been assigned by cve@mitre.org to track the vulnerability - currently rated as HIGH severity.

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
JWT signature validation can be bypassed in versions < 1.3.0 - Issue #3	Third Party Advisory	MISC

JWT signature validation can be bypassed in versions <= 1.3.0 · Issue #3 · FusionAuth/fusionauth-jwt · GitHub	Third Party Advisory github.com text/html	MISC github.com/inversoft/prime-jwt/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	Inversoft	Prime-jwt	All	All	All	All

cpe:2.3:a:inversoft:prime-jwt:*:*:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→