CVE-2016-6298

MITRE | NVD | CVE.ORG | JSON API | Print: PDF

Summary

CVE	CVE-2016-6298
State	PUBLISHED
Assigner	redhat
Source Priority	CVE Program / NVD first with legacy fallback
Published	2016-09-01 23:59:01 UTC
Updated	2026-05-06 22:30:45 UTC
Description	The _Rsa15 class in the RSA 1.5 algorithm implementation in jwa.py in jwcrypto before 0.3.2 lacks the Random Filling prote

Risk And Classification

Primary CVSS: v3.1 5.3 MEDIUM from nvd@nist.gov

CVSS:3.1/AV:N/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N

EPSS: 0.003650000 probability, percentile 0.584780000 (date 2026-05-06)

Problem Types: CWE-200 | n/a

Version	Source	Type	Score	Severity	Vector
3.1	nvd@nist.gov	Primary	5.3	MEDIUM	CVSS:3.1/AV:N/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N
2.0	nvd@nist.gov	Primary	4.3		AV:N/AC:M/Au:N/C:P/I:N/A:N

CVSS v3.1 Breakdown

Attack Vector

Network

Attack Complexity

High

Privileges Required

Low

User Interaction

None

Scope

Unchanged

Confidentiality

High

Integrity

None

Availability

None

CVSS:3.1/AV:N/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N

CVSS v2.0 Breakdown

Access Vector

Network

Access Complexity

Medium

Authentication

None

Confidentiality

Partial

Integrity

None

Availability

None

AV:N/AC:M/Au:N/C:P/I:N/A:N

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Latchset	Jwcrypto	All	All	All	All

Vendor Declared Affected Products

Source	Vendor	Product	Version	Platforms
CNA	Na	N/a	affected n/a	Not specified

References

Reference	Source
JWCrypto CVE-2016-6298 Information Disclosure Vulnerability	af854a3a-2127-422b-91ae-364da2661108
Fix for CVE-2016-6298 by simo5 · Pull Request #66 · latchset/jwcrypto · GitHub	af854a3a-2127-422b-91ae-364da2661108
CVE-2016-6298: Million Messages Attack vulnerability · Issue #65 · latchset/jwcrypto · GitHub	af854a3a-2127-422b-91ae-364da2661108
CVE-2016-6298: Million Messages Attack mitigation · latchset/jwcrypto@eb5be5b · GitHub	af854a3a-2127-422b-91ae-364da2661108
Release Security Release CVE-2016-6298 · latchset/jwcrypto · GitHub	af854a3a-2127-422b-91ae-364da2661108
CVE Program record	CVE.ORG
NVD vulnerability detail	NVD

No vendor comments have been submitted for this CVE.

There are currently no legacy QID mappings associated with this CVE.

Free CVE JSON API cve.report/api

CVE.report and Source URL Uptime Status **status.cve.report**