



# CVE-2016-9121

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

## Summary

<b>CVE</b>	CVE-2016-9121
<b>State</b>	PUBLISHED
<b>Assigner</b>	hackerone
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2017-03-28 02:59:00 UTC
<b>Updated</b>	2025-04-20 01:37:25 UTC
<b>Description</b>	go-jose before 1.0.4 suffers from an invalid curve attack for the ECDH-ES algorithm. When deriving a shared key using EC

## Risk And Classification

**Primary CVSS:** v3.0 9.1 CRITICAL from nvd@nist.gov

**CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:N**

**Problem Types:** CWE-326 | Cryptographic Issue

Version	Source	Type	Score	Severity	Vector
3.0	nvd@nist.gov	Primary	9.1	CRITICAL	<b>CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:N</b>
2.0	nvd@nist.gov	Primary	6.4		<b>AV:N/AC:L/Au:N/C:P/I:P/A:N</b>

## CVSS v3.0 Breakdown

Attack Vector

**Network**

Attack Complexity

**Low**

Privileges Required

**None**

User Interaction

**None**

Scope

**Unchanged**

Confidentiality

**High**

Integrity

**High**

Availability

None

CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:N

### CVSS v2.0 Breakdown

Access Vector

Network

Access Complexity

Low

Authentication

None

Confidentiality

Partial

Integrity

Partial

Availability

None

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

### NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Go-jose Project	Go-jose	All	All	All	All

### Vendor Declared Affected Products

Source	Vendor	Product	Version	Platforms
CNA	Na	Go JOSE All Versions Before 1.0.4	affected Go JOSE All versions before 1.0.4	Not specified

### References

Reference	Source	Link	Tags
HackerOne	af854a3a-2127-422b-91ae-364da2661108	<a href="https://hackerone.com">hackerone.com</a>	Permissi
oss-security - CVE request: multiple issues in go-jose package	af854a3a-2127-422b-91ae-364da2661108	<a href="https://www.openwall.com">www.openwall.com</a>	Mailing L
Merge branch 'cs/164590' · square/go-jose@c758193 · GitHub	af854a3a-2127-422b-91ae-364da2661108	<a href="https://github.com">github.com</a>	Issue Tra
CVE Program record	CVE.ORG	<a href="https://www.cve.org">www.cve.org</a>	canonica
NVD vulnerability detail	NVD	<a href="https://nvd.nist.gov">nvd.nist.gov</a>	canonica

No vendor comments have been submitted for this CVE.

### Legacy QID Mappings

982076 Go (ao) Security Update for aopka.in/square/ao-iose.v1 (GHSA-86r9-39i9-99wp)

© [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](#)