CVE-2016-9121

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

Summary

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

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	CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:N
2.0	nvd@nist.gov	Primary	6.4		AV:N/AC:L/Au:N/C:P/I:P/A:N

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

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

982076 Go (go) Security Update for gopkg.in/square/go-jose.v1 (GHSA-86r9-39j9-99wp)