CVE-2016-9123

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

Summary

CVE	CVE-2016-9123
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 1.0.5 suffers from a CBC-HMAC integer overflow on 32-bit architectures. An integer overflow could lead to a

Risk And Classification

Primary CVSS: v3.0 7.5 HIGH from nvd@nist.gov

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

Problem Types: CWE-190 | Memory Corruption

Version	Source	Type	Score	Severity	Vector
3.0	nvd@nist.gov	Primary	7.5	HIGH	CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:H/A:N
2.0	nvd@nist.gov	Primary	5		AV:N/AC:L/Au:N/C:N/I:P/A:N

CVSS v3.0 Breakdown

Attack Vector

Network

Attack Complexity

Low

Privileges Required

None

User Interaction

None

Scope

Unchanged

Confidentiality

None

Integrity

High

Availability

None

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

CVSS v2.0 Breakdown

Access Vector

Network

Access Complexity

Low

Authentication

None

Confidentiality

None

Integrity

Partial

Availability

None

AV:N/AC:L/Au:N/C:N/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 1.0.5	affected Go JOSE All versions before 1.0.5	Not specified

References

Reference	Source	Link
oss-security - CVE request: multiple issues in go-jose package	af854a3a-2127-422b-91ae-364da2661108	www.oper
HackerOne	af854a3a-2127-422b-91ae-364da2661108	hackeron
Use uint64 for all size calculations, size checks · square/go-jose@789a4c4 · GitHub	af854a3a-2127-422b-91ae-364da2661108	github.co
CVE Program record	CVE.ORG	www.cve.
NVD vulnerability detail	NVD	nvd.nist.g

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

982077 Go (go) Security Update for github.com/square/go-jose (GHSA-3fx4-7f69-5mmq)