# CVE-2016-3959

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

## Summary

| | |
|---|---|
| **CVE** | CVE-2016-3959 |
| **State** | PUBLISHED |
| **Assigner** | mitre |
| **Source Priority** | CVE Program / NVD first with legacy fallback |
| **Published** | 2016-05-23 19:59:04 UTC |
| **Updated** | 2026-05-06 22:30:45 UTC |
| **Description** | The Verify function in crypto/dsa/dsa.go in Go before 1.5.4 and 1.6.x before 1.6.1 does not properly check parameters pass |

## 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:N/A:H

**Problem Types:** CWE-20 | n/a

| 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:N/A:H |
| 2.0 | nvd@nist.gov | Primary | 5 | | AV:N/AC:L/Au:N/C:N/I:N/A:P |

## CVSS v3.0 Breakdown

Attack Vector

Network

Attack Complexity

Low

Privileges Required

None

User Interaction

None

Scope

Unchanged

Confidentiality

None

Integrity

None

Availability

High

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

## CVSS v2.0 Breakdown

Access Vector

Network

Access Complexity

Low

Authentication

None

Confidentiality

None

Integrity

None

Availability

Partial

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

## NVD Known Affected Configurations (CPE 2.3)

| Type | Vendor | Product | Version | Update | Edition | Language |
|---|---|---|---|---|---|---|
| Operating System | Fedoraproject | Fedora | 22 | All | All | All |
| Operating System | Fedoraproject | Fedora | 23 | All | All | All |
| Operating System | Fedoraproject | Fedora | 24 | All | All | All |
| Application | Golang | Go | 1.6 | All | All | All |
| Application | Golang | Go | All | All | All | All |
| Operating System | Opensuse | Leap | 42.1 | All | All | All |

## Vendor Declared Affected Products

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

## References

| Reference | Source | Link |
|---|---|---|
| Google Groups | af854a3a-2127-422b-91ae-364da2661108 | groups.google.com |
| [SECURITY] Fedora 22 Update: golang-1.5.4-1.fc22 | af854a3a-2127-422b-91ae-364da2661108 | lists.fedoraproject.org |
| Gerrit Code Review | af854a3a-2127-422b-91ae-364da2661108 | go-review.googlesource.com |
| oss-security - CVE request - Go - DLL loading, Big int | af854a3a-2127-422b-91ae-364da2661108 | www.openwall.com |
| [SECURITY] Fedora 23 Update: golang-1.5.4-1.fc23 | af854a3a-2127-422b-91ae-364da2661108 | lists.fedoraproject.org |

| | | |
|---|---|---|
| oss-security - Re: CVE request - Go - DLL loading, Big int | af854a3a-2127-422b-91ae-364da2661108 | www.openwall.com |
| Red Hat Customer Portal | af854a3a-2127-422b-91ae-364da2661108 | rhn.redhat.com |
| openSUSE-SU-2016:1331-1: moderate: Security update for go | af854a3a-2127-422b-91ae-364da2661108 | lists.opensuse.org |
| [SECURITY] Fedora 24 Update: golang-1.6.1-1.fc24 | af854a3a-2127-422b-91ae-364da2661108 | lists.fedoraproject.org |
| Google Groups | MITRE | groups.google.com |
| CVE Program record | CVE.ORG | www.cve.org |
| NVD vulnerability detail | NVD | nvd.nist.gov |

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**