



# CVE-2016-2339

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

## Summary

<b>CVE</b>	CVE-2016-2339
<b>State</b>	PUBLISHED
<b>Assigner</b>	certcc
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2017-01-06 21:59:00 UTC
<b>Updated</b>	2026-05-06 22:30:45 UTC
<b>Description</b>	An exploitable heap overflow vulnerability exists in the Fiddle::Function.new "initialize" function functionality of Ruby. In Fiddle::Function.new "initialize" function functionality of Ruby. In Fiddle::Function.new "initialize" function functionality of Ruby.

## Risk And Classification

**Primary CVSS:** v3.0 9.8 CRITICAL from nvd@nist.gov

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

**EPSS:** 0.006840000 probability, percentile 0.717550000 (date 2026-05-11)

**Problem Types:** CWE-119 | heap overflow vulnerability

Version	Source	Type	Score	Severity	Vector
3.0	nvd@nist.gov	Primary	9.8	CRITICAL	CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H
2.0	nvd@nist.gov	Primary	7.5		AV:N/AC:L/Au:N/C:P/I:P/A:P

## CVSS v3.0 Breakdown

Attack Vector

Network

Attack Complexity

Low

Privileges Required

None

User Interaction

None

Scope

Unchanged

Confidentiality

High

Integrity

High

High

Availability

High

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

### CVSS v2.0 Breakdown

Access Vector

Network

Access Complexity

Low

Authentication

None

Confidentiality

Partial

Integrity

Partial

Availability

Partial

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

### NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	<a href="#">Ruby-lang</a>	<a href="#">Ruby</a>	2.2.2	All	All	All
Application	<a href="#">Ruby-lang</a>	<a href="#">Ruby</a>	2.3.0	All	All	All

### Vendor Declared Affected Products

Source	Vendor	Product	Version	Platforms
CNA	<a href="#">Ruby</a>	<a href="#">Ruby</a>	affected 2.3.0 dev	Not specified
CNA	<a href="#">Ruby</a>	<a href="#">Ruby</a>	affected 2.2.2	Not specified

### References

Reference	Source	Link	Tag
[SECURITY] [DLA 1421-1] ruby2.1 security update	af854a3a-2127-422b-91ae-364da2661108	<a href="#">lists.debian.org</a>	
Ruby 'initialize()' Function Heap Buffer Overflow Vulnerability	af854a3a-2127-422b-91ae-364da2661108	<a href="#">www.securityfocus.com</a>	
Cisco Talos - Talos 2016 0034	af854a3a-2127-422b-91ae-364da2661108	<a href="#">www.talosintelligence.com</a>	Exp
CVE Program record	CVE.ORG	<a href="#">www.cve.org</a>	can
NVD vulnerability detail	NVD	<a href="#">nvd.nist.gov</a>	can

No vendor comments have been submitted for this CVE.

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

© [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](#)