



CVE-2013-6371

[MITRE](#)[NVD](#)[CVE.ORG](#)[Print: PDF !\[\]\(e3f8612927870f2e0f9f5989e6dd3064_img.jpg\)](#)

Summary

CVE	CVE-2013-6371
State	PUBLIC
Assigner	secalert@redhat.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2014-04-22 13:06:00 UTC
Updated	2023-09-25 02:30:00 UTC
Description	The hash functionality in json-c before 0.12 allows context-dependent attackers to cause a denial of service (CPU consump

Risk And Classification

Problem Types: CWE-310

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Fedoraproject	Fedora	20	All	All	All
Operating System	Fedoraproject	Fedora	20	All	All	All
Application	Json-c	Json-c	All	All	All	All
Application	Json-c	Json-c	0.1	All	All	All
Application	Json-c	Json-c	0.2	All	All	All
Application	Json-c	Json-c	0.3	All	All	All
Application	Json-c	Json-c	0.4	All	All	All
Application	Json-c	Json-c	0.5	All	All	All
Application	Json-c	Json-c	0.6	All	All	All
Application	Json-c	Json-c	0.7	All	All	All
Application	Json-c	Json-c	0.8	All	All	All
Application	Json-c	Json-c	0.9	All	All	All
Application	Json-c	Json-c	All	All	All	All
Application	Json-c Project	Json-c	0.1	All	All	All
Application	Json-c Project	Json-c	0.10	All	All	All
Application	Json-c Project	Json-c	0.2	All	All	All
Application	Json-c Project	Json-c	0.3	All	All	All

Application	Json-c Project	Json-c	0.4	All	All	All
Application	Json-c Project	Json-c	0.5	All	All	All
Application	Json-c Project	Json-c	0.6	All	All	All
Application	Json-c Project	Json-c	0.7	All	All	All
Application	Json-c Project	Json-c	0.8	All	All	All
Application	Json-c Project	Json-c	0.9	All	All	All
Application	Json-c Project	Json-c	All	All	All	All
Application	Json-c Project	Json-c	0.1	All	All	All
Application	Json-c Project	Json-c	0.10	All	All	All
Application	Json-c Project	Json-c	0.2	All	All	All
Application	Json-c Project	Json-c	0.3	All	All	All
Application	Json-c Project	Json-c	0.4	All	All	All
Application	Json-c Project	Json-c	0.5	All	All	All
Application	Json-c Project	Json-c	0.6	All	All	All
Application	Json-c Project	Json-c	0.7	All	All	All
Application	Json-c Project	Json-c	0.8	All	All	All
Application	Json-c Project	Json-c	0.9	All	All	All

References

Reference	Source	Link	Tags
1032311 – (CVE-2013-6371) CVE-2013-6371 json-c: hash collision DoS	CONFIRM	bugzilla.redhat.com	Issue
Support / Security / Advisories // MDVSA-2014:079 Mandriva	MANDRIVA	www.mandriva.com	Broken
Oracle Solaris Third Party Bulletin - October 2015	CONFIRM	www.oracle.com	Third Party
Patch to address the following issues: · 64e3690 · json-c/json-c · GitHub	CONFIRM	github.com	Issue
[SECURITY] Fedora 20 Update: json-c-0.11-6.fc20	FEDORA	lists.fedoraproject.org	Third Party
IBM X-Force Exchange	XF	exchange.xforce.ibmcloud.com	
Malformed Request	BID	www.securityfocus.com	Third Party
Security Advisory SA57791 - JSON-C Two Denial of Service Vulnerabilities - Secunia	SECUNIA	secunia.com	Permission
CVE Program record	CVE.ORG	www.cve.org	Canonical
NVD vulnerability detail	NVD	nvd.nist.gov	Canonical

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](#).

CVE.report and Source URL Uptime Status [status.cve.report](#)