



CVE-2010-3611

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

Summary

CVE	CVE-2010-3611
State	PUBLIC
Assigner	cert@cert.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2010-11-04 18:00:00 UTC
Updated	2017-08-17 01:33:00 UTC
Description	ISC DHCP server 4.0 before 4.0.2, 4.1 before 4.1.2, and 4.2 before 4.2.0-P1 allows remote attackers to cause a denial of s

Risk And Classification

Problem Types: NVD-CWE-Other

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	isc	Dhcp	4.0	All	All	All
Application	isc	Dhcp	4.0.0	All	All	All
Application	isc	Dhcp	4.0.1	All	All	All
Application	isc	Dhcp	4.0.1	b1	All	All
Application	isc	Dhcp	4.0.1	rc1	All	All
Application	isc	Dhcp	4.1.0	All	All	All
Application	isc	Dhcp	4.1.1	All	All	All
Application	isc	Dhcp	4.1.1	b1	All	All
Application	isc	Dhcp	4.1.1	b2	All	All
Application	isc	Dhcp	4.1.1	b3	All	All
Application	isc	Dhcp	4.1.1	rc1	All	All
Application	isc	Dhcp	4.2.0	All	All	All
Application	isc	Dhcp	4.2.0	a1	All	All
Application	isc	Dhcp	4.2.0	a2	All	All
Application	isc	Dhcp	4.2.0	b1	All	All
Application	isc	Dhcp	4.2.0	b2	All	All
Application	isc	Dhcp	4.2.0	rc1	All	All

Application	Isc	Dhcp	4.0	All	All	All
Application	Isc	Dhcp	4.0.0	All	All	All
Application	Isc	Dhcp	4.0.1	All	All	All
Application	Isc	Dhcp	4.0.1	b1	All	All
Application	Isc	Dhcp	4.0.1	rc1	All	All
Application	Isc	Dhcp	4.1.0	All	All	All
Application	Isc	Dhcp	4.1.1	All	All	All
Application	Isc	Dhcp	4.1.1	b1	All	All
Application	Isc	Dhcp	4.1.1	b2	All	All
Application	Isc	Dhcp	4.1.1	b3	All	All
Application	Isc	Dhcp	4.1.1	rc1	All	All
Application	Isc	Dhcp	4.2.0	All	All	All
Application	Isc	Dhcp	4.2.0	a1	All	All
Application	Isc	Dhcp	4.2.0	a2	All	All
Application	Isc	Dhcp	4.2.0	b1	All	All
Application	Isc	Dhcp	4.2.0	b2	All	All
Application	Isc	Dhcp	4.2.0	rc1	All	All

References						
Reference				Source	Link	
[security-announce] SUSE Security Summary Report: SUSE-SR:2010:021				SUSE	lists.opensus	
CERT Vulnerability Notes Database				CERT-VN	www.kb.cert.	
Webmail : Solution de messagerie professionnelle - OVHcloud- OVH				VUPEN	www.vupen.c	
Webmail : Solution de messagerie professionnelle - OVHcloud- OVH				VUPEN	www.vupen.c	
68999				OSVDB	osvdb.org	
Security Advisory SA42407 - Red Hat update for dhcp - Secunia				SECUNIA	secunia.com	
Webmail : Solution de messagerie professionnelle - OVHcloud- OVH				VUPEN	www.vupen.c	
IBM X-Force Exchange				XF	exchange.xfc	
[SECURITY] Fedora 13 Update: dhcp-4.1.1-27.P1.fc13				FEDORA	lists.fedorapr	
DHCP: Server Crash with Empty Link-Address Field Internet Systems Consortium				CONFIRM	www.isc.org	
Security Advisory SA42345 - Fedora update for dhcp - Secunia				SECUNIA	secunia.com	
Support / Security / Advisories // MDVSA-2010:226 Mandriva				MANDRIVA	www.mandriva	
ISC DHCP Relay-Forward Denial of Service Vulnerability - Advisories - Community				SECUNIA	secunia.com	
ISC DHCP Server Relay-Forward Empty Link-Address Field Denial of Service Vulnerability				BID	www.security	
649877 – (CVE-2010-3611) CVE-2010-3611 dhcp: NULL pointer dereference crash via crafted DHCPv6 packet				CONFIRM	bugzilla.redh	

Support	REDHAT	www.redhat.com
[SECURITY] Fedora 14 Update: dhcp-4.2.0-14.P1.fc14	FEDORA	lists.fedoraproject.org
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.

© 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