



CVE-2010-3616

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

Summary

CVE	CVE-2010-3616
State	PUBLIC
Assigner	cert@cert.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2010-12-17 19:00:00 UTC
Updated	2011-01-19 07:00:00 UTC
Description	ISC DHCP server 4.2 before 4.2.0-P2, when configured to use failover partnerships, allows remote attackers to cause a denial of service (DHCP server crash) by sending a malformed packet to the server.

Risk And Classification

Problem Types: CWE-20

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	isc	Dhcp	4.2.0	All	All	All
Application	isc	Dhcp	4.2.0	p1	All	All
Application	isc	Dhcp	4.2.0	All	All	All
Application	isc	Dhcp	4.2.0	p1	All	All

References

Reference	Source	Link	Tags
Support / Security / Advisories // MDVSA-2011:001 Mandriva	MANDRIVA	www.mandriva.com	
Webmail : Solution de messagerie professionnelle - OVHcloud- OVH	VUPEN	www.vupen.com	
DHCP: Server Hangs with TCP to Failover Peer Port Internet Systems Consortium	CONFIRM	www.isc.org	Vendor Advisory
US-CERT Vulnerability Note VU#159528	CERT-VN	www.kb.cert.org	US Government
Webmail : Solution de messagerie professionnelle - OVHcloud- OVH	VUPEN	www.vupen.com	Vendor Advisory
Fedora update for dhcp - Advisories - Community	SECUNIA	secunia.com	
[SECURITY] Fedora 14 Update: dhcp-4.2.0-16.P2.fc14	FEDORA	lists.fedoraproject.org	
nagios check_tcp kills failover, then dhcp failure.	MLIST	lists.isc.org	
ISC DHCP Server Failover Peer Port Field Denial of Service Vulnerability	BID	www.securityfocus.com	
SecurityTracker: ISC DHCP TCP Failover Bug Lets Remote Users Deny Service	SECTRACK	www.securitytracker.com	

ISC DHCP Failover Peer Denial of Service Vulnerability - Advisories - Community	SECUNIA	secunia.com	Vendor Adv
CVE Program record	CVE.ORG	www.cve.org	canonical
NVD vulnerability detail	NVD	nvd.nist.gov	canonical, a

No vendor comments have been submitted for this CVE.

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

© [CVE.report](https://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](https://mitre.org) and the authoritative source of CVE content is [MITRE's CVE web site](https://mitre.org/cve). 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