



# CVE-2012-3954

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

## Summary

<b>CVE</b>	CVE-2012-3954
<b>State</b>	PUBLIC
<b>Assigner</b>	cve@mitre.org
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2012-07-25 10:42:00 UTC
<b>Updated</b>	2020-04-01 13:59:00 UTC
<b>Description</b>	Multiple memory leaks in ISC DHCP 4.1.x and 4.2.x before 4.2.4-P1 and 4.1-ESV before 4.1-ESV-R6 allow remote attacker

## Risk And Classification

### Problem Types: CWE-399

## NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	<a href="#">Canonical</a>	<a href="#">Ubuntu Linux</a>	11.04	All	All	All
Operating System	<a href="#">Canonical</a>	<a href="#">Ubuntu Linux</a>	11.10	All	All	All
Operating System	<a href="#">Canonical</a>	<a href="#">Ubuntu Linux</a>	12.04	All	All	All
Operating System	<a href="#">Canonical</a>	<a href="#">Ubuntu Linux</a>	11.04	All	All	All
Operating System	<a href="#">Canonical</a>	<a href="#">Ubuntu Linux</a>	11.10	All	All	All
Operating System	<a href="#">Canonical</a>	<a href="#">Ubuntu Linux</a>	12.04	All	All	All
Operating System	<a href="#">Debian</a>	<a href="#">Debian Linux</a>	6.0	All	All	All
Operating System	<a href="#">Debian</a>	<a href="#">Debian Linux</a>	7.0	All	All	All
Operating System	<a href="#">Debian</a>	<a href="#">Debian Linux</a>	6.0	All	All	All
Operating System	<a href="#">Debian</a>	<a href="#">Debian Linux</a>	7.0	All	All	All
Application	<a href="#">isc</a>	<a href="#">Dhcp</a>	4.1-esv	-	All	All
Application	<a href="#">isc</a>	<a href="#">Dhcp</a>	4.1-esv	r1	All	All
Application	<a href="#">isc</a>	<a href="#">Dhcp</a>	4.1-esv	r2	All	All
Application	<a href="#">isc</a>	<a href="#">Dhcp</a>	4.1-esv	r3	All	All
Application	<a href="#">isc</a>	<a href="#">Dhcp</a>	4.1-esv	r3_b1	All	All
Application	<a href="#">isc</a>	<a href="#">Dhcp</a>	4.1-esv	r4	All	All
Application	<a href="#">isc</a>	<a href="#">Dhcp</a>	4.1-esv	r5	All	All

Application	lsc	Dhcp	4.1-esv	r5_b1	All	All
Application	lsc	Dhcp	4.1-esv	r5_rc1	All	All
Application	lsc	Dhcp	4.1-esv	r5_rc2	All	All
Application	lsc	Dhcp	4.1-esv	rc1	All	All
Application	lsc	Dhcp	4.1.0	-	All	All
Application	lsc	Dhcp	4.1.0	a1	All	All
Application	lsc	Dhcp	4.1.0	a2	All	All
Application	lsc	Dhcp	4.1.0	b1	All	All
Application	lsc	Dhcp	4.1.1	-	All	All
Application	lsc	Dhcp	4.1.1	b1	All	All
Application	lsc	Dhcp	4.1.1	b2	All	All
Application	lsc	Dhcp	4.1.1	b3	All	All
Application	lsc	Dhcp	4.1.1	rc1	All	All
Application	lsc	Dhcp	4.1.2	-	All	All
Application	lsc	Dhcp	4.1.2	b1	All	All
Application	lsc	Dhcp	4.1.2	p1	All	All
Application	lsc	Dhcp	4.1.2	rc1	All	All
Application	lsc	Dhcp	4.2.0	-	All	All
Application	lsc	Dhcp	4.2.0	a1	All	All
Application	lsc	Dhcp	4.2.0	a2	All	All
Application	lsc	Dhcp	4.2.0	b1	All	All
Application	lsc	Dhcp	4.2.0	b2	All	All
Application	lsc	Dhcp	4.2.0	p1	All	All
Application	lsc	Dhcp	4.2.0	rc1	All	All
Application	lsc	Dhcp	4.2.1	-	All	All
Application	lsc	Dhcp	4.2.1	b1	All	All
Application	lsc	Dhcp	4.2.1	rc1	All	All
Application	lsc	Dhcp	4.2.2	-	All	All
Application	lsc	Dhcp	4.2.2	b1	All	All
Application	lsc	Dhcp	4.2.2	rc1	All	All
Application	lsc	Dhcp	4.2.3	-	All	All
Application	lsc	Dhcp	4.2.3	p1	All	All
Application	lsc	Dhcp	4.2.3	p2	All	All
Application	lsc	Dhcp	4.2.4	All	All	All
Application	lsc	Dhcp	4.1-esv	-	All	All

Application	isc	Dhcp	4.1-esv	r1	All	All
Application	isc	Dhcp	4.1-esv	r2	All	All
Application	isc	Dhcp	4.1-esv	r3	All	All
Application	isc	Dhcp	4.1-esv	r3_b1	All	All
Application	isc	Dhcp	4.1-esv	r4	All	All
Application	isc	Dhcp	4.1-esv	r5	All	All
Application	isc	Dhcp	4.1-esv	r5_b1	All	All
Application	isc	Dhcp	4.1-esv	r5_rc1	All	All
Application	isc	Dhcp	4.1-esv	r5_rc2	All	All
Application	isc	Dhcp	4.1-esv	rc1	All	All
Application	isc	Dhcp	4.1.0	-	All	All
Application	isc	Dhcp	4.1.0	a1	All	All
Application	isc	Dhcp	4.1.0	a2	All	All
Application	isc	Dhcp	4.1.0	b1	All	All
Application	isc	Dhcp	4.1.1	-	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	4.1.2	-	All	All
Application	isc	Dhcp	4.1.2	b1	All	All
Application	isc	Dhcp	4.1.2	p1	All	All
Application	isc	Dhcp	4.1.2	rc1	All	All
Application	isc	Dhcp	4.2.0	-	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	p1	All	All
Application	isc	Dhcp	4.2.0	rc1	All	All
Application	isc	Dhcp	4.2.1	-	All	All
Application	isc	Dhcp	4.2.1	b1	All	All
Application	isc	Dhcp	4.2.1	rc1	All	All
Application	isc	Dhcp	4.2.2	-	All	All
Application	isc	Dhcp	4.2.2	b1	All	All

Application	isc	Dhcp	4.2.2	rc1	All	All
Application	isc	Dhcp	4.2.3	-	All	All
Application	isc	Dhcp	4.2.3	p1	All	All
Application	isc	Dhcp	4.2.3	p2	All	All
Application	isc	Dhcp	4.2.4	All	All	All

## References

Reference	Source	Link
USN-1519-1: DHCP vulnerabilities   Ubuntu	UBUNTU	<a href="http://www.ubuntu.com">www.ubuntu.com</a>
ISC DHCP Multiple Denial of Service Vulnerabilities	BID	<a href="http://www.securityfocus.com">www.securityfocus.com</a>
CVE-2012-3954: Memory Leaks Found in ISC DHCP   Internet Systems Consortium Knowledge Base	CONFIRM	<a href="http://kb.isc.org">kb.isc.org</a>
openSUSE-SU-2012:1006-1: moderate: update for dhcp	SUSE	<a href="http://lists.opensuse.org">lists.opensuse.org</a>
Support / Security / Advisories // MDVSA-2012:116   Mandriva	MANDRIVA	<a href="http://www.mandriva.com">www.mandriva.com</a>
Support / Security / Advisories // MDVSA-2012:115   Mandriva	MANDRIVA	<a href="http://www.mandriva.com">www.mandriva.com</a>
Debian -- Security Information -- DSA-2519-2 isc-dhcp	DEBIAN	<a href="http://www.debian.org">www.debian.org</a>
Red Hat Customer Portal	REDHAT	<a href="http://rhn.redhat.com">rhn.redhat.com</a>
Gentoo Linux Documentation -- ISC DHCP: Denial of Service	GENTOO	<a href="http://security.gentoo.org">security.gentoo.org</a>
ISC DHCP Memory Leak Lets Remote Users Deny Service - SecurityTracker	SECTRACK	<a href="http://www.securitytracker.com">www.securitytracker.com</a>
Debian -- Security Information -- DSA-2516-1 isc-dhcp	DEBIAN	<a href="http://www.debian.org">www.debian.org</a>
CVE Program record	CVE.ORG	<a href="http://www.cve.org">www.cve.org</a>
NVD vulnerability detail	NVD	<a href="http://nvd.nist.gov">nvd.nist.gov</a>

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](http://www.mitre.org) and the authoritative source of CVE content is [MITRE's CVE web site](http://www.mitre.org). This site includes MITRE data granted under the following [license](http://www.mitre.org).

**CVE.report and Source URL Uptime Status** [status.cve.report](http://status.cve.report)