



CVE-2022-2928

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

Summary

CVE	CVE-2022-2928
State	PUBLIC
Assigner	security-officer@isc.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2022-10-07 05:15:00 UTC
Updated	2023-11-07 03:47:00 UTC
Description	In ISC DHCP 4.4.0 -> 4.4.3, ISC DHCP 4.1-ESV-R1 -> 4.1-ESV-R16-P1, when the function option_code_hash_lookup() is c

Risk And Classification

Problem Types: CWE-476

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Debian	Debian Linux	10.0	All	All	All
Operating System	Fedoraproject	Fedora	35	All	All	All
Operating System	Fedoraproject	Fedora	36	All	All	All
Operating System	Fedoraproject	Fedora	37	All	All	All
Application	isc	Dhcp	4.1-esv	r1	All	All
Application	isc	Dhcp	4.1-esv	r10	All	All
Application	isc	Dhcp	4.1-esv	r10b1	All	All
Application	isc	Dhcp	4.1-esv	r10rc1	All	All
Application	isc	Dhcp	4.1-esv	r10_b1	All	All
Application	isc	Dhcp	4.1-esv	r10_rc1	All	All
Application	isc	Dhcp	4.1-esv	r11	All	All
Application	isc	Dhcp	4.1-esv	r11b1	All	All
Application	isc	Dhcp	4.1-esv	r11rc1	All	All
Application	isc	Dhcp	4.1-esv	r11rc2	All	All
Application	isc	Dhcp	4.1-esv	r11_b1	All	All
Application	isc	Dhcp	4.1-esv	r11_rc1	All	All
Application	isc	Dhcp	4.1-esv	r11_rc2	All	All

Application	isc	Dhcp	4.1-esv	r12	All	All
Application	isc	Dhcp	4.1-esv	r12-p1	All	All
Application	isc	Dhcp	4.1-esv	r12b1	All	All
Application	isc	Dhcp	4.1-esv	r12_b1	All	All
Application	isc	Dhcp	4.1-esv	r12_p1	All	All
Application	isc	Dhcp	4.1-esv	r13	All	All
Application	isc	Dhcp	4.1-esv	r13b1	All	All
Application	isc	Dhcp	4.1-esv	r13_b1	All	All
Application	isc	Dhcp	4.1-esv	r14	All	All
Application	isc	Dhcp	4.1-esv	r14b1	All	All
Application	isc	Dhcp	4.1-esv	r14_b1	All	All
Application	isc	Dhcp	4.1-esv	r15	All	All
Application	isc	Dhcp	4.1-esv	r15-p1	All	All
Application	isc	Dhcp	4.1-esv	r15_b1	All	All
Application	isc	Dhcp	4.1-esv	r16	All	All
Application	isc	Dhcp	4.1-esv	r16-p1	All	All
Application	isc	Dhcp	All	All	All	All

References

Reference	Source	Link	Tag
[SECURITY] Fedora 37 Update: dhcp-4.4.3-4.P1.fc37 - package-announce - Fedora Mailing-Lists		lists.fedoraproject.org	
[SECURITY] Fedora 36 Update: dhcp-4.4.3-4.P1.fc36 - package-announce - Fedora Mailing-Lists	FEDORA	lists.fedoraproject.org	
ISC DHCP: Multiple Vulnerabilities (GLSA 202305-22) — Gentoo security	GENTOO	security.gentoo.org	
[SECURITY] Fedora 36 Update: dhcp-4.4.3-4.P1.fc36 - package-announce - Fedora Mailing-Lists		lists.fedoraproject.org	
[SECURITY] Fedora 35 Update: dhcp-4.4.3-4.P1.fc35 - package-announce - Fedora Mailing-Lists	FEDORA	lists.fedoraproject.org	
[SECURITY] Fedora 35 Update: dhcp-4.4.3-4.P1.fc35 - package-announce - Fedora Mailing-Lists		lists.fedoraproject.org	
cve-website	MISC	www.cve.org	
[SECURITY] [DLA 3146-1] isc-dhcp security update	MLIST	lists.debian.org	
[SECURITY] Fedora 37 Update: dhcp-4.4.3-4.P1.fc37 - package-announce - Fedora Mailing-Lists	FEDORA	lists.fedoraproject.org	
CVE-2022-2928 An option refcount overflow exists in dhcpd	CONFIRM	kb.isc.org	
NVD vulnerability detail	NVD	nvd.nist.gov	can

Vendor Comments And Credit

Discovery Credit

LEGACY: ISC would like to thank VictorV of Cyber Kunlun Lab for discovering and reporting this issue

Legacy QID Mappings

[160628](#) Oracle Enterprise Linux Security Update for dhcp security and enhancement update (ELSA-2023-2502)

[160661](#) Oracle Enterprise Linux Security Update for dhcp (ELSA-2023-3000)

[181114](#) Debian Security Update for isc-dhcp (DSA 5251-1)

[181126](#) Debian Security Update for isc-dhcp (DLA 3146-1)

[183928](#) Debian Security Update for isc-dhcp (CVE-2022-2928)

[198973](#) Ubuntu Security Notification for DHCP Vulnerabilities (USN-5658-1)

[241461](#) Red Hat Update for dhcp (RHSA-2023:2502)

[241476](#) Red Hat Update for dhcp (RHSA-2023:3000)

[283204](#) Fedora Security Update for dhcp (FEDORA-2022-f5a45757df)

[283244](#) Fedora Security Update for dhcp (FEDORA-2022-c4f274a54f)

[283485](#) Fedora Security Update for dhcp (FEDORA-2022-9ca9a94e28)

[354111](#) Amazon Linux Security Advisory for dhcp : ALAS2-2022-1874

[355050](#) Amazon Linux Security Advisory for dhcp : AL2012-2022-374

[378641](#) Alibaba Cloud Linux Security Update for dhcp (ALINUX3-SA-2023:0058)

[502519](#) Alpine Linux Security Update for dhcp

[503675](#) Alpine Linux Security Update for dhcp

[505866](#) Alpine Linux Security Update for dhcp

[591311](#) Bosch Rexroth PRA-ES8P2S Ethernet-Switch Multiple Vulnerabilities (BOSCH-SA-247053-BT)

[672402](#) EulerOS Security Update for dhcp (EulerOS-SA-2022-2792)

[672424](#) EulerOS Security Update for dhcp (EulerOS-SA-2022-2842)

[672461](#) EulerOS Security Update for dhcp (EulerOS-SA-2022-2817)

[672477](#) EulerOS Security Update for dhcp (EulerOS-SA-2023-1032)

[672510](#) EulerOS Security Update for dhcp (EulerOS-SA-2023-1007)

[672529](#) EulerOS Security Update for dhcp (EulerOS-SA-2023-1097)

[672557](#) EulerOS Security Update for dhcp (EulerOS-SA-2023-1121)

[672744](#) EulerOS Security Update for dhcp (EulerOS-SA-2023-1498)

710726 Gentoo Linux ISC DHCP Multiple Vulnerabilities (GLSA 202305-22)
752801 SUSE Enterprise Linux Security Update for dhcp (SUSE-SU-2022:3992-1)
752802 SUSE Enterprise Linux Security Update for dhcp (SUSE-SU-2022:3991-1)
904199 Common Base Linux Mariner (CBL-Mariner) Security Update for dhcp (11110)
904218 Common Base Linux Mariner (CBL-Mariner) Security Update for dhcp (11108)
941056 AlmaLinux Security Update for dhcp (ALSA-2023:2502)
941097 AlmaLinux Security Update for dhcp (ALSA-2023:3000)

© [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](#)