



# CVE-2022-2929

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

## Summary

|                        |   |
|------------------------|---|
| <b>CVE</b>             | CVE-2022-2929   |
| <b>State</b>           | PUBLIC  |
| <b>Assigner</b>        | security-officer@isc.org  |
| <b>Source Priority</b> | CVE Program / NVD first with legacy fallback  |
| <b>Published</b>       | 2022-10-07 05:15:00 UTC   |
| <b>Updated</b>         | 2023-11-07 03:47:00 UTC   |
| <b>Description</b>     | In ISC DHCP 1.0 -> 4.4.3, ISC DHCP 4.1-ESV-R1 -> 4.1-ESV-R16-P1 a system with access to a DHCP server, sending Dh |

## Risk And Classification

**Problem Types:** CWE-770

## NVD Known Affected Configurations (CPE 2.3)

| Type             | Vendor                        | Product                      | Version | Update  | Edition | Language |
|------------------|-------------------------------|------------------------------|---------|---------|---------|----------|
| Operating System | <a href="#">Debian</a>        | <a href="#">Debian Linux</a> | 10.0    | All     | All     | All      |
| Operating System | <a href="#">Fedoraproject</a> | <a href="#">Fedora</a>       | 35      | All     | All     | All      |
| Operating System | <a href="#">Fedoraproject</a> | <a href="#">Fedora</a>       | 36      | All     | All     | All      |
| Operating System | <a href="#">Fedoraproject</a> | <a href="#">Fedora</a>       | 37      | All     | All     | All      |
| Application      | <a href="#">isc</a>           | <a href="#">Dhcp</a>         | All     | All     | 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 | r10     | All     | All      |
| Application      | <a href="#">isc</a>           | <a href="#">Dhcp</a>         | 4.1-esv | r10b1   | All     | All      |
| Application      | <a href="#">isc</a>           | <a href="#">Dhcp</a>         | 4.1-esv | r10rc1  | All     | All      |
| Application      | <a href="#">isc</a>           | <a href="#">Dhcp</a>         | 4.1-esv | r10_b1  | All     | All      |
| Application      | <a href="#">isc</a>           | <a href="#">Dhcp</a>         | 4.1-esv | r10_rc1 | All     | All      |
| Application      | <a href="#">isc</a>           | <a href="#">Dhcp</a>         | 4.1-esv | r11     | All     | All      |
| Application      | <a href="#">isc</a>           | <a href="#">Dhcp</a>         | 4.1-esv | r11b1   | All     | All      |
| Application      | <a href="#">isc</a>           | <a href="#">Dhcp</a>         | 4.1-esv | r11rc1  | All     | All      |
| Application      | <a href="#">isc</a>           | <a href="#">Dhcp</a>         | 4.1-esv | r11rc2  | All     | All      |
| Application      | <a href="#">isc</a>           | <a href="#">Dhcp</a>         | 4.1-esv | r11_b1  | All     | All      |
| Application      | <a href="#">isc</a>           | <a href="#">Dhcp</a>         | 4.1-esv | r11_rc1 | All     | All      |

|             |                     |                      |         |         |     |     |
|-------------|---------------------|----------------------|---------|---------|-----|-----|
| Application | <a href="#">isc</a> | <a href="#">Dhcp</a> | 4.1-esv | r11_rc2 | All | All |
| Application | <a href="#">isc</a> | <a href="#">Dhcp</a> | 4.1-esv | r12     | All | All |
| Application | <a href="#">isc</a> | <a href="#">Dhcp</a> | 4.1-esv | r12-p1  | All | All |
| Application | <a href="#">isc</a> | <a href="#">Dhcp</a> | 4.1-esv | r12b1   | All | All |
| Application | <a href="#">isc</a> | <a href="#">Dhcp</a> | 4.1-esv | r12_b1  | All | All |
| Application | <a href="#">isc</a> | <a href="#">Dhcp</a> | 4.1-esv | r12_p1  | All | All |
| Application | <a href="#">isc</a> | <a href="#">Dhcp</a> | 4.1-esv | r13     | All | All |
| Application | <a href="#">isc</a> | <a href="#">Dhcp</a> | 4.1-esv | r13b1   | All | All |
| Application | <a href="#">isc</a> | <a href="#">Dhcp</a> | 4.1-esv | r13_b1  | All | All |
| Application | <a href="#">isc</a> | <a href="#">Dhcp</a> | 4.1-esv | r14     | All | All |
| Application | <a href="#">isc</a> | <a href="#">Dhcp</a> | 4.1-esv | r14b1   | All | All |
| Application | <a href="#">isc</a> | <a href="#">Dhcp</a> | 4.1-esv | r14_b1  | All | All |
| Application | <a href="#">isc</a> | <a href="#">Dhcp</a> | 4.1-esv | r15     | All | All |
| Application | <a href="#">isc</a> | <a href="#">Dhcp</a> | 4.1-esv | r15-p1  | All | All |
| Application | <a href="#">isc</a> | <a href="#">Dhcp</a> | 4.1-esv | r15_b1  | All | All |
| Application | <a href="#">isc</a> | <a href="#">Dhcp</a> | 4.1-esv | r16     | All | All |
| Application | <a href="#">isc</a> | <a href="#">Dhcp</a> | 4.1-esv | r16-p1  | All | All |
| Application | <a href="#">isc</a> | <a href="#">Dhcp</a> | 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 |         | <a href="https://lists.fedoraproject.org">lists.fedoraproject.org</a> |     |
| [SECURITY] Fedora 36 Update: dhcp-4.4.3-4.P1.fc36 - package-announce - Fedora Mailing-Lists | FEDORA  | <a href="https://lists.fedoraproject.org">lists.fedoraproject.org</a> |     |
| ISC DHCP: Multiple Vulnerabilities (GLSA 202305-22) — Gentoo security                       | GENTOO  | <a href="https://security.gentoo.org">security.gentoo.org</a>         |     |
| [SECURITY] Fedora 36 Update: dhcp-4.4.3-4.P1.fc36 - package-announce - Fedora Mailing-Lists |         | <a href="https://lists.fedoraproject.org">lists.fedoraproject.org</a> |     |
| [SECURITY] Fedora 35 Update: dhcp-4.4.3-4.P1.fc35 - package-announce - Fedora Mailing-Lists | FEDORA  | <a href="https://lists.fedoraproject.org">lists.fedoraproject.org</a> |     |
| [SECURITY] Fedora 35 Update: dhcp-4.4.3-4.P1.fc35 - package-announce - Fedora Mailing-Lists |         | <a href="https://lists.fedoraproject.org">lists.fedoraproject.org</a> |     |
| [SECURITY] [DLA 3146-1] isc-dhcp security update  | MLIST   | <a href="https://lists.debian.org">lists.debian.org</a>               |     |
| [SECURITY] Fedora 37 Update: dhcp-4.4.3-4.P1.fc37 - package-announce - Fedora Mailing-Lists | FEDORA  | <a href="https://lists.fedoraproject.org">lists.fedoraproject.org</a> |     |
| CVE-2022-2929 DHCP memory leak  | CONFIRM | <a href="https://kb.isc.org">kb.isc.org</a>                           |     |
| cve-website   | MISC    | <a href="https://www.cve.org">www.cve.org</a>                         |     |
| NVD vulnerability detail  | NVD     | <a href="https://nvd.nist.gov">nvd.nist.gov</a>                       | 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)

[182170](#) Debian Security Update for isc-dhcp (CVE-2022-2929)

[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-2023-1400)

|   |
|---|
| <a href="#">672744</a> EulerOS Security Update for dnchp (EulerOS-SA-2023-1498)                 |
| <a href="#">710726</a> Gentoo Linux ISC DHCP Multiple Vulnerabilities (GLSA 202305-22)          |
| <a href="#">752801</a> SUSE Enterprise Linux Security Update for dhcp (SUSE-SU-2022:3992-1)     |
| <a href="#">752802</a> SUSE Enterprise Linux Security Update for dhcp (SUSE-SU-2022:3991-1)     |
| <a href="#">904194</a> Common Base Linux Mariner (CBL-Mariner) Security Update for dhcp (11111) |
| <a href="#">904217</a> Common Base Linux Mariner (CBL-Mariner) Security Update for dhcp (11109) |
| <a href="#">941056</a> AlmaLinux Security Update for dhcp (ALSA-2023:2502)                      |
| <a href="#">941097</a> 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](#)**