



# CVE-2018-5732

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

## Summary

<b>CVE</b>	CVE-2018-5732
<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>	2019-10-09 16:15:00 UTC
<b>Updated</b>	2020-01-09 21:14:00 UTC
<b>Description</b>	Failure to properly bounds-check a buffer used for processing DHCP options allows a malicious server (or an entity masquer

## Risk And Classification

### Problem Types: CWE-119

## NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
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	-	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	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	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	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	r14	All	All
Application	<a href="#">isc</a>	<a href="#">Dhcp</a>	4.1-esv	r14b1	All	All

Application	<a href="#">lsc</a>	<a href="#">Dhcp</a>	4.1-esv	r15	All	All
Application	<a href="#">lsc</a>	<a href="#">Dhcp</a>	4.1-esv	r2	All	All
Application	<a href="#">lsc</a>	<a href="#">Dhcp</a>	4.1-esv	r3	All	All
Application	<a href="#">lsc</a>	<a href="#">Dhcp</a>	4.1-esv	r3b1	All	All
Application	<a href="#">lsc</a>	<a href="#">Dhcp</a>	4.1-esv	r4	All	All
Application	<a href="#">lsc</a>	<a href="#">Dhcp</a>	4.1-esv	r5	All	All
Application	<a href="#">lsc</a>	<a href="#">Dhcp</a>	4.1-esv	r5b1	All	All
Application	<a href="#">lsc</a>	<a href="#">Dhcp</a>	4.1-esv	r5rc1	All	All
Application	<a href="#">lsc</a>	<a href="#">Dhcp</a>	4.1-esv	r5rc2	All	All
Application	<a href="#">lsc</a>	<a href="#">Dhcp</a>	4.1-esv	r6	All	All
Application	<a href="#">lsc</a>	<a href="#">Dhcp</a>	4.1-esv	r7	All	All
Application	<a href="#">lsc</a>	<a href="#">Dhcp</a>	4.1-esv	r8	All	All
Application	<a href="#">lsc</a>	<a href="#">Dhcp</a>	4.1-esv	r8b1	All	All
Application	<a href="#">lsc</a>	<a href="#">Dhcp</a>	4.1-esv	r8rc1	All	All
Application	<a href="#">lsc</a>	<a href="#">Dhcp</a>	4.1-esv	r9	All	All
Application	<a href="#">lsc</a>	<a href="#">Dhcp</a>	4.1-esv	r9b1	All	All
Application	<a href="#">lsc</a>	<a href="#">Dhcp</a>	4.1-esv	r9rc1	All	All
Application	<a href="#">lsc</a>	<a href="#">Dhcp</a>	4.1.2	p1	All	All
Application	<a href="#">lsc</a>	<a href="#">Dhcp</a>	4.4.0	All	All	All
Application	<a href="#">lsc</a>	<a href="#">Dhcp</a>	All	All	All	All
Application	<a href="#">lsc</a>	<a href="#">Dhcp</a>	4.1-esv	-	All	All
Application	<a href="#">lsc</a>	<a href="#">Dhcp</a>	4.1-esv	r1	All	All
Application	<a href="#">lsc</a>	<a href="#">Dhcp</a>	4.1-esv	r10	All	All
Application	<a href="#">lsc</a>	<a href="#">Dhcp</a>	4.1-esv	r10b1	All	All
Application	<a href="#">lsc</a>	<a href="#">Dhcp</a>	4.1-esv	r10rc1	All	All
Application	<a href="#">lsc</a>	<a href="#">Dhcp</a>	4.1-esv	r11	All	All
Application	<a href="#">lsc</a>	<a href="#">Dhcp</a>	4.1-esv	r11b1	All	All
Application	<a href="#">lsc</a>	<a href="#">Dhcp</a>	4.1-esv	r11rc1	All	All
Application	<a href="#">lsc</a>	<a href="#">Dhcp</a>	4.1-esv	r11rc2	All	All
Application	<a href="#">lsc</a>	<a href="#">Dhcp</a>	4.1-esv	r12	All	All
Application	<a href="#">lsc</a>	<a href="#">Dhcp</a>	4.1-esv	r12-p1	All	All
Application	<a href="#">lsc</a>	<a href="#">Dhcp</a>	4.1-esv	r12b1	All	All
Application	<a href="#">lsc</a>	<a href="#">Dhcp</a>	4.1-esv	r13	All	All
Application	<a href="#">lsc</a>	<a href="#">Dhcp</a>	4.1-esv	r13b1	All	All
Application	<a href="#">lsc</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	r15	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	r3b1	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	<a href="#">isc</a>	<a href="#">Dhcp</a>	4.1-esv	r5b1	All	All
Application	<a href="#">isc</a>	<a href="#">Dhcp</a>	4.1-esv	r5rc1	All	All
Application	<a href="#">isc</a>	<a href="#">Dhcp</a>	4.1-esv	r5rc2	All	All
Application	<a href="#">isc</a>	<a href="#">Dhcp</a>	4.1-esv	r6	All	All
Application	<a href="#">isc</a>	<a href="#">Dhcp</a>	4.1-esv	r7	All	All
Application	<a href="#">isc</a>	<a href="#">Dhcp</a>	4.1-esv	r8	All	All
Application	<a href="#">isc</a>	<a href="#">Dhcp</a>	4.1-esv	r8b1	All	All
Application	<a href="#">isc</a>	<a href="#">Dhcp</a>	4.1-esv	r8rc1	All	All
Application	<a href="#">isc</a>	<a href="#">Dhcp</a>	4.1-esv	r9	All	All
Application	<a href="#">isc</a>	<a href="#">Dhcp</a>	4.1-esv	r9b1	All	All
Application	<a href="#">isc</a>	<a href="#">Dhcp</a>	4.1-esv	r9rc1	All	All
Application	<a href="#">isc</a>	<a href="#">Dhcp</a>	4.1.2	p1	All	All
Application	<a href="#">isc</a>	<a href="#">Dhcp</a>	4.4.0	All	All	All
Application	<a href="#">isc</a>	<a href="#">Dhcp</a>	All	All	All	All

## References

Reference	Source	Link	Tags
CVE-2018-5732: Potential buffer overflow	CONFIRM	<a href="https://kb.isc.org">kb.isc.org</a>	Vendor Advisory
CVE Program record	CVE.ORG	<a href="https://www.cve.org">www.cve.org</a>	canonical
NVD vulnerability detail	NVD	<a href="https://nvd.nist.gov">nvd.nist.gov</a>	canonical, analysis

## Vendor Comments And Credit

### Discovery Credit

**LEGACY:** ISC would like to thank Felix Wilhelm, Google Security Team, for reporting this vulnerability.

## Legacy QID Mappings

[500145](#) Alpine Linux Security Update for dhcp

[503795](#) Alpine Linux Security Update for dhcp

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

710315 Gentoo Linux ISC DHCP Multiple Vulnerabilities (GLSA 201804-05)

© [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](#)**