# CVE-2018-5733

MITRE | NVD | CVE.ORG | Print: PDF

## Summary

| | |
|---|---|
| **CVE** | CVE-2018-5733 |
| **State** | PUBLIC |
| **Assigner** | security-officer@isc.org |
| **Source Priority** | CVE Program / NVD first with legacy fallback |
| **Published** | 2019-01-16 20:29:00 UTC |
| **Updated** | 2020-01-09 21:08:00 UTC |
| **Description** | A malicious client which is allowed to send very large amounts of traffic (billions of packets) to a DHCP server can eventual |

## Risk And Classification

**Problem Types:** CWE-190

## NVD Known Affected Configurations (CPE 2.3)

| Type | Vendor | Product | Version | Update | Edition | Language |
|---|---|---|---|---|---|---|
| Operating System | Canonical | Ubuntu Linux | 14.04 | All | All | All |
| Operating System | Canonical | Ubuntu Linux | 16.04 | All | All | All |
| Operating System | Canonical | Ubuntu Linux | 17.10 | All | All | All |
| Operating System | Canonical | Ubuntu Linux | 14.04 | All | All | All |
| Operating System | Canonical | Ubuntu Linux | 16.04 | All | All | All |
| Operating System | Canonical | Ubuntu Linux | 17.10 | All | All | All |
| Operating System | Debian | Debian Linux | 7.0 | All | All | All |
| Operating System | Debian | Debian Linux | 8.0 | All | All | All |
| Operating System | Debian | Debian Linux | 9.0 | All | All | All |
| Operating System | Debian | Debian Linux | 7.0 | All | All | All |
| Operating System | Debian | Debian Linux | 8.0 | All | All | All |
| Operating System | Debian | Debian Linux | 9.0 | All | All | All |
| Application | Isc | Dhcp | 4.1-esv | - | 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 | 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 | 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_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 | r13_b1 | All | All |
| Application | Isc | Dhcp | 4.1-esv | r14 | 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 | 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 | r6 | All | All |
| Application | Isc | Dhcp | 4.1-esv | r7 | All | All |
| Application | Isc | Dhcp | 4.1-esv | r8 | All | All |
| Application | Isc | Dhcp | 4.1-esv | r8_b1 | All | All |
| Application | Isc | Dhcp | 4.1-esv | r8_rc1 | All | All |
| Application | Isc | Dhcp | 4.1-esv | r9 | All | All |
| Application | Isc | Dhcp | 4.1-esv | r9_b1 | All | All |
| Application | Isc | Dhcp | 4.1-esv | r9_rc1 | All | All |
| Application | Isc | Dhcp | 4.1-esv | rc1 | All | All |
| Application | Isc | Dhcp | 4.1.0 | - | All | All |
| Application | Isc | Dhcp | 4.4.0 | All | All | All |
| Application | Isc | Dhcp | 4.1-esv | - | 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 | 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 | 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_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 | r13_b1 | All | All |
| Application | Isc | Dhcp | 4.1-esv | r14 | 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 | 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 | r6 | All | All |
| Application | Isc | Dhcp | 4.1-esv | r7 | All | All |
| Application | Isc | Dhcp | 4.1-esv | r8 | All | All |
| Application | Isc | Dhcp | 4.1-esv | r8_b1 | All | All |
| Application | Isc | Dhcp | 4.1-esv | r8_rc1 | All | All |
| Application | Isc | Dhcp | 4.1-esv | r9 | All | All |
| Application | Isc | Dhcp | 4.1-esv | r9_b1 | All | All |
| Application | Isc | Dhcp | 4.1-esv | r9_rc1 | All | All |
| Application | Isc | Dhcp | 4.1-esv | rc1 | All | All |
| Application | Isc | Dhcp | 4.1.0 | - | All | All |
| Application | Isc | Dhcp | 4.4.0 | All | All | All |
| Application | Isc | Dhcp | All | All | All | All |
| Application | Isc | Dhcp | All | All | All | All |
| Operating System | Redhat | Enterprise Linux Desktop | 6.0 | All | All | All |

| | | | | | | |
|---|---|---|---|---|---|---|
| Operating System | Redhat | Enterprise Linux Desktop | 7.0 | All | All | All |
| Operating System | Redhat | Enterprise Linux Desktop | 6.0 | All | All | All |
| Operating System | Redhat | Enterprise Linux Desktop | 7.0 | All | All | All |
| Operating System | Redhat | Enterprise Linux Server | 6.0 | All | All | All |
| Operating System | Redhat | Enterprise Linux Server | 7.0 | All | All | All |
| Operating System | Redhat | Enterprise Linux Server | 6.0 | All | All | All |
| Operating System | Redhat | Enterprise Linux Server | 7.0 | All | All | All |
| Operating System | Redhat | Enterprise Linux Server Aus | 7.4 | All | All | All |
| Operating System | Redhat | Enterprise Linux Server Aus | 7.6 | All | All | All |
| Operating System | Redhat | Enterprise Linux Server Aus | 7.4 | All | All | All |
| Operating System | Redhat | Enterprise Linux Server Aus | 7.6 | All | All | All |
| Operating System | Redhat | Enterprise Linux Server Eus | 7.4 | All | All | All |
| Operating System | Redhat | Enterprise Linux Server Eus | 7.5 | All | All | All |
| Operating System | Redhat | Enterprise Linux Server Eus | 7.6 | All | All | All |
| Operating System | Redhat | Enterprise Linux Server Eus | 7.4 | All | All | All |
| Operating System | Redhat | Enterprise Linux Server Eus | 7.5 | All | All | All |
| Operating System | Redhat | Enterprise Linux Server Eus | 7.6 | All | All | All |
| Operating System | Redhat | Enterprise Linux Workstation | 6.0 | All | All | All |
| Operating System | Redhat | Enterprise Linux Workstation | 7.0 | All | All | All |
| Operating System | Redhat | Enterprise Linux Workstation | 6.0 | All | All | All |
| Operating System | Redhat | Enterprise Linux Workstation | 7.0 | All | All | All |

## References

| Reference | Source | Link |
|---|---|---|
| Red Hat Customer Portal | REDHAT | access.re |
| ISC DHCP CVE-2018-5733 Remote Denial of Service Vulnerability | BID | www.secu |
| Security Advisories-CVE-2018-5733: A malicious client can overflow a reference counter in ISC dhcpd | CONFIRM | kb.isc.org |
| Red Hat Customer Portal | REDHAT | access.re |
| [SECURITY] [DLA 1313-1] isc-dhcp security update | MLIST | lists.debia |
| USN-3586-1: DHCP vulnerabilities \| Ubuntu security notices \| Ubuntu | UBUNTU | usn.ubun |
| Dhcp Reference Counter Overflow Lets Remote Users Cause the Target dhcpd Service to Crash - SecurityTracker | SECTRACK | www.secu |
| USN-3586-2: DHCP vulnerabilities \| Ubuntu security notices | UBUNTU | usn.ubun |
| Debian -- Security Information -- DSA-4133-1 isc-dhcp | DEBIAN | www.deb |
| CVE Program record | CVE.ORG | www.cve. |
| NVD vulnerability detail | NVD | nvd.nist.g |

## 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

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