



CVE-2017-3144

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

Summary

| | |
|------------------------|---|
| CVE | CVE-2017-3144 |
| 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 21:07:00 UTC |
| Description | A vulnerability stemming from failure to properly clean up closed OMAPI connections can lead to exhaustion of the pool of s |

Risk And Classification

Problem Types: CWE-400

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 | 8.0 | All | All | All |
| Operating System | Debian | Debian Linux | 9.0 | 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 | lsc | Dhcp | 4.1-esv | r11_rc1 | All | All |
| Application | lsc | Dhcp | 4.1-esv | r11_rc2 | All | All |
| Application | lsc | Dhcp | 4.1-esv | r12 | All | All |
| Application | lsc | Dhcp | 4.1-esv | r12_b1 | All | All |
| Application | lsc | Dhcp | 4.1-esv | r12_p1 | All | All |
| Application | lsc | Dhcp | 4.1-esv | r13 | All | All |
| Application | lsc | Dhcp | 4.1-esv | r13_b1 | All | All |
| Application | lsc | Dhcp | 4.1-esv | r14 | All | All |
| Application | lsc | Dhcp | 4.1-esv | r14_b1 | All | All |
| Application | lsc | Dhcp | 4.1-esv | r15 | All | All |
| Application | lsc | Dhcp | 4.1-esv | r2 | All | All |
| Application | lsc | Dhcp | 4.1-esv | r3 | All | All |
| Application | lsc | Dhcp | 4.1-esv | r3_b1 | All | All |
| Application | lsc | Dhcp | 4.1-esv | r4 | All | All |
| Application | lsc | Dhcp | 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 | r6 | All | All |
| Application | lsc | Dhcp | 4.1-esv | r7 | All | All |
| Application | lsc | Dhcp | 4.1-esv | r8 | All | All |
| Application | lsc | Dhcp | 4.1-esv | r8_b1 | All | All |
| Application | lsc | Dhcp | 4.1-esv | r8_rc1 | All | All |
| Application | lsc | Dhcp | 4.1-esv | r9 | All | All |
| Application | lsc | Dhcp | 4.1-esv | r9_b1 | All | All |
| Application | lsc | Dhcp | 4.1-esv | r9_rc1 | All | All |
| Application | lsc | Dhcp | 4.1.0 | All | All | All |
| Application | lsc | Dhcp | 4.1-esv | - | All | All |
| Application | lsc | Dhcp | 4.1-esv | r1 | All | All |
| Application | lsc | Dhcp | 4.1-esv | r10 | All | All |
| Application | lsc | Dhcp | 4.1-esv | r10_b1 | All | All |
| Application | lsc | Dhcp | 4.1-esv | r10_rc1 | All | All |
| Application | lsc | Dhcp | 4.1-esv | r11 | All | All |
| Application | lsc | Dhcp | 4.1-esv | r11_b1 | All | All |
| Application | lsc | Dhcp | 4.1-esv | r11_rc1 | All | All |

| | | | | | | |
|------------------|--------|-----------------------------|---------|---------|-----|-----|
| Application | lsc | Dhcp | 4.1-esv | r11_rc2 | All | All |
| Application | lsc | Dhcp | 4.1-esv | r12 | All | All |
| Application | lsc | Dhcp | 4.1-esv | r12_b1 | All | All |
| Application | lsc | Dhcp | 4.1-esv | r12_p1 | All | All |
| Application | lsc | Dhcp | 4.1-esv | r13 | All | All |
| Application | lsc | Dhcp | 4.1-esv | r13_b1 | All | All |
| Application | lsc | Dhcp | 4.1-esv | r14 | All | All |
| Application | lsc | Dhcp | 4.1-esv | r14_b1 | All | All |
| Application | lsc | Dhcp | 4.1-esv | r15 | All | All |
| Application | lsc | Dhcp | 4.1-esv | r2 | All | All |
| Application | lsc | Dhcp | 4.1-esv | r3 | All | All |
| Application | lsc | Dhcp | 4.1-esv | r3_b1 | All | All |
| Application | lsc | Dhcp | 4.1-esv | r4 | All | All |
| Application | lsc | Dhcp | 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 | r6 | All | All |
| Application | lsc | Dhcp | 4.1-esv | r7 | All | All |
| Application | lsc | Dhcp | 4.1-esv | r8 | All | All |
| Application | lsc | Dhcp | 4.1-esv | r8_b1 | All | All |
| Application | lsc | Dhcp | 4.1-esv | r8_rc1 | All | All |
| Application | lsc | Dhcp | 4.1-esv | r9 | All | All |
| Application | lsc | Dhcp | 4.1-esv | r9_b1 | All | All |
| Application | lsc | Dhcp | 4.1-esv | r9_rc1 | All | All |
| Application | lsc | Dhcp | 4.1.0 | All | All | All |
| Application | lsc | Dhcp | All | All | All | All |
| Application | lsc | Dhcp | All | All | All | All |
| Operating System | Redhat | Enterprise Linux Desktop | 7.0 | All | All | All |
| Operating System | Redhat | Enterprise Linux Desktop | 7.0 | All | All | All |
| Operating System | Redhat | Enterprise Linux Server | 7.0 | 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 | Hedhat | 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 Server Tus | 7.4 | All | All | All |
| Operating System | Redhat | Enterprise Linux Server Tus | 7.6 | All | All | All |
| Operating System | Redhat | Enterprise Linux Server Tus | 7.4 | All | All | All |
| Operating System | Redhat | Enterprise Linux Server Tus | 7.6 | All | All | All |
| Operating System | Redhat | Enterprise Linux Workstation | 7.0 | All | All | All |
| Operating System | Redhat | Enterprise Linux Workstation | 7.0 | All | All | All |

References

Reference

[Red Hat Customer Portal](#)

[Security Advisories-CVE-2017-3144: Failure to properly clean up closed OMAPI connections can exhaust available sockets](#)

[ISC DHCP CVE-2017-3144 Remote Denial of Service Vulnerability](#)

[ISC DHCP OMAPI Connection Management Flaw Lets Remote Users Consume Excessive Socket Descriptors on the Target System - Security](#)

[USN-3586-1: DHCP vulnerabilities | Ubuntu security notices | Ubuntu](#)

[Debian -- Security Information -- DSA-4133-1 isc-dhcp](#)

[CVE Program record](#)

[NVD vulnerability detail](#)

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

[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](#)