



# CVE-2018-1000115

[MITRE](#)[NVD](#)[CVE.ORG](#)[Print: PDF !\[\]\(e3f8612927870f2e0f9f5989e6dd3064\_img.jpg\)](#)

## Summary

<b>CVE</b>	CVE-2018-1000115
<b>State</b>	PUBLIC
<b>Assigner</b>	cve@mitre.org
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2018-03-05 14:29:00 UTC
<b>Updated</b>	2021-08-04 17:15:00 UTC
<b>Description</b>	Memcached version 1.5.5 contains an Insufficient Control of Network Message Volume (Network Amplification, CWE-406) \

## Risk And Classification

### Problem Types: CWE-400

## NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	<a href="#">Canonical</a>	<a href="#">Ubuntu Linux</a>	14.04	All	All	All
Operating System	<a href="#">Canonical</a>	<a href="#">Ubuntu Linux</a>	16.04	All	All	All
Operating System	<a href="#">Canonical</a>	<a href="#">Ubuntu Linux</a>	17.10	All	All	All
Operating System	<a href="#">Canonical</a>	<a href="#">Ubuntu Linux</a>	14.04	All	All	All
Operating System	<a href="#">Canonical</a>	<a href="#">Ubuntu Linux</a>	16.04	All	All	All
Operating System	<a href="#">Canonical</a>	<a href="#">Ubuntu Linux</a>	17.10	All	All	All
Operating System	<a href="#">Debian</a>	<a href="#">Debian Linux</a>	8.0	All	All	All
Operating System	<a href="#">Debian</a>	<a href="#">Debian Linux</a>	9.0	All	All	All
Operating System	<a href="#">Debian</a>	<a href="#">Debian Linux</a>	8.0	All	All	All
Operating System	<a href="#">Debian</a>	<a href="#">Debian Linux</a>	9.0	All	All	All
Application	<a href="#">Memcached</a>	<a href="#">Memcached</a>	1.5.5	All	All	All
Application	<a href="#">Memcached</a>	<a href="#">Memcached</a>	1.5.5	All	All	All
Application	<a href="#">Redhat</a>	<a href="#">Openstack</a>	10	All	All	All
Application	<a href="#">Redhat</a>	<a href="#">Openstack</a>	10.0	All	All	All
Application	<a href="#">Redhat</a>	<a href="#">Openstack</a>	11	All	All	All
Application	<a href="#">Redhat</a>	<a href="#">Openstack</a>	11.0	All	All	All
Application	<a href="#">Redhat</a>	<a href="#">Openstack</a>	12	All	All	All

Application	<a href="#">Redhat</a>	<a href="#">Openstack</a>	12.0	All	All	All
Application	<a href="#">Redhat</a>	<a href="#">Openstack</a>	8	All	All	All
Application	<a href="#">Redhat</a>	<a href="#">Openstack</a>	8.0	All	All	All
Application	<a href="#">Redhat</a>	<a href="#">Openstack</a>	9	All	All	All
Application	<a href="#">Redhat</a>	<a href="#">Openstack</a>	9.0	All	All	All
Application	<a href="#">Redhat</a>	<a href="#">Openstack</a>	10.0	All	All	All
Application	<a href="#">Redhat</a>	<a href="#">Openstack</a>	11.0	All	All	All
Application	<a href="#">Redhat</a>	<a href="#">Openstack</a>	12.0	All	All	All
Application	<a href="#">Redhat</a>	<a href="#">Openstack</a>	8.0	All	All	All
Application	<a href="#">Redhat</a>	<a href="#">Openstack</a>	9.0	All	All	All

## References

### Reference

[ReleaseNotes156 · memcached/memcached Wiki · GitHub](#)

[Memcached-fueled 1.3 Tbps attacks - The Akamai Blog](#)

[Red Hat Customer Portal](#)

[UDP Amplification Attacks, result of Memcached UDP port 11211 · Issue #348 · memcached/memcached · GitHub](#)

[Red Hat Customer Portal](#)

[Red Hat Customer Portal](#)

[Memcached 1.5.5 - 'Memcrashed' Insufficient Control Network Message Volume Denial of Service \(1\) - Linux dos Exploit](#)

[Synology Inc.](#)

[Red Hat Customer Portal](#)

[dormando on Twitter: "For what it's worth, if you're getting attacked by memcached's, it's pretty easy to disable them since the source won't be](#)

[Debian -- Security Information -- DSA-4218-1 memcached](#)

[Memcached 1.5.5 - 'Memcrashed ' Insufficient Control of Network Message Volume Denial of Service With Shodan API - Linux dos Exploit](#)

[USN-3588-1: Memcached vulnerabilities | Ubuntu security notices | Ubuntu](#)

[disable UDP port by default · memcached/memcached@dbb7a8a · GitHub](#)

[Red Hat Customer Portal](#)

[CVE Program record](#)

[NVD vulnerability detail](#)



No vendor comments have been submitted for this CVE.

## Legacy QID Mappings

[296090 Oracle Solaris 11.4 Support Repository Update \(SRU\) 5.1.3 Missing \(CPUJAN2019\)](#)

671070 EulerOS Security Update for memcached (EulerOS-SA-2019-2631)

671098 EulerOS Security Update for memcached (EulerOS-SA-2019-2213)

© [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](#)**