



# CVE-2019-10192

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

## Summary

<b>CVE</b>	CVE-2019-10192
<b>State</b>	PUBLIC
<b>Assigner</b>	secalert@redhat.com
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2019-07-11 19:15:00 UTC
<b>Updated</b>	2021-10-28 12:14:00 UTC
<b>Description</b>	A heap-buffer overflow vulnerability was found in the Redis hyperloglog data structure versions 3.x before 3.2.13, 4.x before

## Risk And Classification

**Problem Types:** CWE-787

## 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>	16.04	All	All	All
Operating System	<a href="#">Canonical</a>	<a href="#">Ubuntu Linux</a>	18.04	All	All	All
Operating System	<a href="#">Canonical</a>	<a href="#">Ubuntu Linux</a>	19.04	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>	18.04	All	All	All
Operating System	<a href="#">Canonical</a>	<a href="#">Ubuntu Linux</a>	19.04	All	All	All
Operating System	<a href="#">Debian</a>	<a href="#">Debian Linux</a>	10.0	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>	10.0	All	All	All
Operating System	<a href="#">Debian</a>	<a href="#">Debian Linux</a>	9.0	All	All	All
Application	<a href="#">Oracle</a>	<a href="#">Communications Operations Monitor</a>	3.4	All	All	All
Application	<a href="#">Oracle</a>	<a href="#">Communications Operations Monitor</a>	4.1	All	All	All
Operating System	<a href="#">Redhat</a>	<a href="#">Enterprise Linux</a>	8.0	All	All	All
Operating System	<a href="#">Redhat</a>	<a href="#">Enterprise Linux</a>	8.0	All	All	All
Operating System	<a href="#">Redhat</a>	<a href="#">Enterprise Linux Eus</a>	8.1	All	All	All
Operating System	<a href="#">Redhat</a>	<a href="#">Enterprise Linux Eus</a>	8.2	All	All	All
Operating System	<a href="#">Redhat</a>	<a href="#">Enterprise Linux Eus</a>	8.4	All	All	All

Operating System	Redhat	Enterprise Linux Server Aus	8.2	All	All	All
Operating System	Redhat	Enterprise Linux Server Aus	8.4	All	All	All
Operating System	Redhat	Enterprise Linux Server Tus	8.2	All	All	All
Operating System	Redhat	Enterprise Linux Server Tus	8.4	All	All	All
Application	Redhat	Openstack	10	All	All	All
Application	Redhat	Openstack	13	All	All	All
Application	Redhat	Openstack	13.0	All	All	All
Application	Redhat	Openstack	14	All	All	All
Application	Redhat	Openstack	14.0	All	All	All
Application	Redhat	Openstack	9	All	All	All
Application	Redhat	Openstack	9.0	All	All	All
Application	Redhat	Openstack	10	All	All	All
Application	Redhat	Openstack	13.0	All	All	All
Application	Redhat	Openstack	14.0	All	All	All
Application	Redhat	Openstack	9.0	All	All	All
Application	Redhat	Software Collections	1.0	All	All	All
Application	Redislabs	Redis	All	All	All	All
Application	Redislabs	Redis	All	All	All	All

## References

Reference	Source	Link
1723918 – (CVE-2019-10192) CVE-2019-10192 redis: Heap buffer overflow in HyperLogLog triggered by malicious client	CONFIRM	<a href="#">bug</a>
Oracle Critical Patch Update Advisory - July 2020	MISC	<a href="#">www</a>
Red Hat Customer Portal - Access to 24x7 support and knowledge	REDHAT	<a href="#">acce</a>
Debian -- Security Information -- DSA-4480-1 redis	DEBIAN	<a href="#">www</a>
Redis Multiple Buffer Overflow Vulnerabilities	BID	<a href="#">www</a>
Red Hat Customer Portal	REDHAT	<a href="#">acce</a>
Red Hat Customer Portal - Access to 24x7 support and knowledge	REDHAT	<a href="#">acce</a>
Red Hat Customer Portal - Access to 24x7 support and knowledge	REDHAT	<a href="#">acce</a>
Red Hat Customer Portal	REDHAT	<a href="#">acce</a>
<a href="https://raw.githubusercontent.com/antirez/redis/3.2/00-RELEASENOTES">raw.githubusercontent.com/antirez/redis/3.2/00-RELEASENOTES</a>	MISC	<a href="#">raw.</a>
Bugtraq: [SECURITY] [DSA 4480-1] redis security update	BUGTRAQ	<a href="#">secl</a>
Red Hat Customer Portal	REDHAT	<a href="#">acce</a>
<a href="https://raw.githubusercontent.com/antirez/redis/4.0/00-RELEASENOTES">raw.githubusercontent.com/antirez/redis/4.0/00-RELEASENOTES</a>	MISC	<a href="#">raw.</a>
Redis: Multiple vulnerabilities (GLSA 201908-04) — Gentoo security	GENTOO	<a href="#">secu</a>
<a href="#">https://raw.githubusercontent.com/antirez/redis/5.0/00-RELEASENOTES</a>	MISC	

raw.githubusercontent.com/antirez/redis/5.0/00-RELEASENOTES	MISC	<a href="#">raw.</a>
USN-4061-1: Redis vulnerabilities   Ubuntu security notices	UBUNTU	<a href="#">usn.</a>
Red Hat Customer Portal	REDHAT	<a href="#">acco</a>
CVE Program record	CVE.ORG	<a href="#">www</a>
NVD vulnerability detail	NVD	<a href="#">nvd.</a>

No vendor comments have been submitted for this CVE.

### Legacy QID Mappings

<a href="#">500602</a> Alpine Linux Security Update for redis
<a href="#">504350</a> Alpine Linux Security Update for redis
<a href="#">710155</a> Gentoo Linux Redis Multiple vulnerabilities (GLSA 201908-04)
<a href="#">960797</a> Rocky Linux Security Update for redis:5 (RLSA-2019:2002)

© [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](#)**