



CVE-2021-3531

[MITRE](#)[NVD](#)[CVE.ORG](#)[Print: PDF !\[\]\(e3f8612927870f2e0f9f5989e6dd3064_img.jpg\)](#)

Summary

CVE	CVE-2021-3531
State	PUBLIC
Assigner	secalert@redhat.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2021-05-18 12:15:00 UTC
Updated	2023-11-07 03:38:00 UTC
Description	A flaw was found in the Red Hat Ceph Storage RGW in versions before 14.2.21. When processing a GET Request for a sw

Risk And Classification

Problem Types: CWE-617

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Fedoraproject	Fedora	32	All	All	All
Operating System	Fedoraproject	Fedora	33	All	All	All
Operating System	Fedoraproject	Fedora	34	All	All	All
Application	Redhat	Ceph	All	All	All	All
Application	Redhat	Ceph Storage	4.0	All	All	All

References

Reference	Source	Link	Tags
[SECURITY] Fedora 34 Update: ceph-16.2.4-1.fc34 - package-announce - Fedora Mailing-Lists	FEDORA	lists.fedoraproject.org	
[SECURITY] Fedora 33 Update: ceph-15.2.12-1.fc33 - package-announce - Fedora Mailing-Lists	FEDORA	lists.fedoraproject.org	
[SECURITY] [DLA 3629-1] ceph security update	MLIST	lists.debian.org	
[SECURITY] Fedora 33 Update: ceph-15.2.12-1.fc33 - package-announce - Fedora Mailing-Lists		lists.fedoraproject.org	
[SECURITY] Fedora 34 Update: ceph-16.2.4-1.fc34 - package-announce - Fedora Mailing-Lists		lists.fedoraproject.org	
[SECURITY] Fedora 32 Update: ceph-14.2.21-1.fc32 - package-announce - Fedora Mailing-Lists		lists.fedoraproject.org	
oss-security - Re: CVE-2021-3531: Ceph: RGW unauthenticated denial of service	MLIST	www.openwall.com	
oss-security - CVE-2021-3531: Ceph: RGW unauthenticated denial of service	MLIST	www.openwall.com	
[SECURITY] Fedora 32 Update: ceph-14.2.21-1.fc32 - package-announce - Fedora Mailing-Lists	FEDORA	lists.fedoraproject.org	

1955326 – (CVE-2021-3531) CVE-2021-3531 ceph: RGW unauthenticated denial of service	MISC	bugzilla.redhat.com	
CVE Program record	CVE.ORG	www.cve.org	cano
NVD vulnerability detail	NVD	nvd.nist.gov	cano

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

- [180341](#) Debian Security Update for ceph (CVE-2021-3531)
- [198423](#) Ubuntu Security Notification for Ceph vulnerabilities (USN-4998-1)
- [198554](#) Ubuntu Security Notification for Ceph Vulnerabilities (USN-5128-1)
- [240201](#) Red Hat Update for kernel-rt (RHSA-2022:1199)
- [281145](#) Fedora Security Update for ceph (FEDORA-2021-6e540b85b9)
- [281146](#) Fedora Security Update for ceph (FEDORA-2021-1bf13db941)
- [281147](#) Fedora Security Update for ceph (FEDORA-2021-ec414c5e18)
- [501811](#) Alpine Linux Security Update for ceph
- [502829](#) Alpine Linux Security Update for ceph16
- [6000278](#) Debian Security Update for ceph (DLA 3629-1)
- [670530](#) EulerOS Security Update for ceph (EulerOS-SA-2021-2288)
- [750099](#) SUSE Enterprise Linux Security Update for ceph (SUSE-SU-2021:1834-1)
- [750100](#) SUSE Enterprise Linux Security Update for ceph (SUSE-SU-2021:1835-1)
- [750174](#) OpenSUSE Security Update for ceph (openSUSE-SU-2021:0833-1)
- [750795](#) OpenSUSE Security Update for ceph (openSUSE-SU-2021:1834-1)

© [CVE.report](https://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](https://mitre.org) and the authoritative source of CVE content is [MITRE's CVE web site](https://mitre.org/cve). This site includes MITRE data granted under the following [license](#).

CVE.report and Source URL Uptime Status status.cve.report