



CVE-2022-3650

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

Summary

CVE	CVE-2022-3650
State	PUBLIC
Assigner	secalert@redhat.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2023-01-17 19:15:00 UTC
Updated	2023-12-23 10:15:00 UTC
Description	A privilege escalation flaw was found in Ceph. Ceph-crash.service allows a local attacker to escalate privileges to root in the

Risk And Classification

Problem Types: NVD-CWE-noinfo

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Redhat	Ceph	16.2.9	All	All	All

References

Reference	Source	Link	Tags
[SECURITY] Fedora 36 Update: ceph-16.2.12-1.fc36 - package-announce - Fedora Mailing-Lists	MISC	lists.fedoraproject.org	
oss-sec: ceph: ceph-crash.service allows local ceph user to root exploit (CVE-2022-3650)	MISC	seclists.org	
Ceph: Root Privilege Escalation (GLSA 202312-10) — Gentoo security		security.gentoo.org	
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

- [183627](#) Debian Security Update for ceph (CVE-2022-3650)
- [199326](#) Ubuntu Security Notification for Ceph Vulnerabilities (USN-6063-1)
- [199662](#) Ubuntu Security Notification for Ceph Vulnerability (USN-6292-1)

[241216](#) Red Hat Update for red hat ceph storage 5.3 bug fix and (RHSA-2023:0980)

[283935](#) Fedora Security Update for ceph (FEDORA-2023-d6b219d19a)

[710814](#) Gentoo Linux Ceph Root Privilege Escalation Vulnerability (GLSA 202312-10)

[753847](#) SUSE Enterprise Linux Security Update for ceph (SUSE-SU-2023:1580-1)

© [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](#)