CVE-2020-12059

MITRE | NVD | CVE.ORG | Print: PDF

Summary

CVE	CVE-2020-12059
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2020-04-22 13:15:00 UTC
Updated	2023-10-23 19:15:00 UTC
Description	An issue was discovered in Ceph through 13.2.9. A POST request with an invalid tagging XML can crash the RGW process

Risk And Classification

Problem Types: CWE-476

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Canonical	Ubuntu Linux	16.04	All	All	All
Operating System	Canonical	Ubuntu Linux	18.04	All	All	All
Application	Linuxfoundation	Ceph	All	All	All	All

References

Reference	Source	Link
[SECURITY] [DLA 3629-1] ceph security update	MLIST	lists.debian.or
USN-4528-1: Ceph vulnerabilities | Ubuntu security notices | Ubuntu	UBUNTU	usn.ubuntu.cc
Bug 1170170 – VUL-0: ceph: specially crafted XML payload on POST requests can crash RGW leading to DOS	MISC	bugzilla.suse.
Bug #44967: rgw:rgw crash when putting object tagging and post object with malformedXML - rgw - Ceph	MISC	tracker.ceph.c
13.1.0 — Ceph Documentation	MISC	docs.ceph.cor
CVE Program record	CVE.ORG	www.cve.org
NVD vulnerability detail	NVD	nvd.nist.gov

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

6000278 Debian Security Update for ceph (DLA 3629-1)