CVE-2018-1128

MITRE | NVD | CVE.ORG | Print: PDF

Summary

CVE	CVE-2018-1128
State	PUBLIC
Assigner	secalert@redhat.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2018-07-10 14:29:00 UTC
Updated	2020-11-17 19:15:00 UTC
Description	It was found that cephx authentication protocol did not verify ceph clients correctly and was vulnerable to replay attack. Any

Risk And Classification

Problem Types: CWE-287

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Debian	Debian Linux	8.0	All	All	All
Operating System	Debian	Debian Linux	9.0	All	All	All
Operating System	Debian	Debian Linux	8.0	All	All	All
Operating System	Debian	Debian Linux	9.0	All	All	All
Operating System	Opensuse	Leap	15.0	All	All	All
Operating System	Opensuse	Leap	15.0	All	All	All
Application	Redhat	Ceph	All	All	All	All
Application	Redhat	Ceph Storage	3	All	All	All
Application	Redhat	Ceph Storage	3	All	All	All
Application	Redhat	Ceph Storage Mon	2	All	All	All
Application	Redhat	Ceph Storage Mon	3	All	All	All
Application	Redhat	Ceph Storage Mon	2	All	All	All
Application	Redhat	Ceph Storage Mon	3	All	All	All
Application	Redhat	Ceph Storage Osd	2	All	All	All
Application	Redhat	Ceph Storage Osd	3	All	All	All
Application	Redhat	Ceph Storage Osd	2	All	All	All
Application	Redhat	Ceph Storage Osd	3	All	All	All

Operating System	Redhat	Enterprise Linux	7.0	All	All	All
Operating System	Redhat	Enterprise Linux	7.0	All	All	All
Operating System	Redhat	Enterprise Linux Desktop	7.0	All	All	All
Operating System	Redhat	Enterprise Linux Desktop	7.0	All	All	All
Operating System	Redhat	Enterprise Linux Server	7.0	All	All	All
Operating System	Redhat	Enterprise Linux Server	7.0	All	All	All
Operating System	Redhat	Enterprise Linux Workstation	7.0	All	All	All
Operating System	Redhat	Enterprise Linux Workstation	7.0	All	All	All

References

Reference	Source	Link	Tags
Bug #24836: auth: cephx authorizer subject to replay - RADOS - Ceph	CONFIRM	tracker.ceph.com	Issue T
Red Hat Customer Portal	REDHAT	access.redhat.com	Third P
auth/cephx: add authorizer challenge · ceph/ceph@5ead971 · GitHub	CONFIRM	github.com	Patch,
Red Hat Customer Portal	REDHAT	access.redhat.com	Third P
[SECURITY] [DLA 1715-1] linux-4.9 security update	MLIST	lists.debian.org	Mailing
[security-announce] openSUSE-SU-2019:1284-1: moderate: Security update f	SUSE	lists.opensuse.org	Third P
Debian -- Security Information -- DSA-4339-1 ceph	DEBIAN	www.debian.org	Third P
Red Hat Customer Portal	REDHAT	access.redhat.com	Third P
oss-security - Re: CVE-2020-25677 ceph: CEPHX_V2 replay attack protection lost	MLIST	www.openwall.com	
Red Hat Customer Portal	REDHAT	access.redhat.com	Third P
1575866 – (CVE-2018-1128) CVE-2018-1128 ceph: cephx protocol is vulnerable to replay attack	CONFIRM	bugzilla.redhat.com	Issue T
oss-security - CVE-2020-25677 ceph: CEPHX_V2 replay attack protection lost	MLIST	www.openwall.com	
CVE Program record	CVE.ORG	www.cve.org	canoni
NVD vulnerability detail	NVD	nvd.nist.gov	canoni

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

671703 EulerOS Security Update for kernel (EulerOS-SA-2022-1735)

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