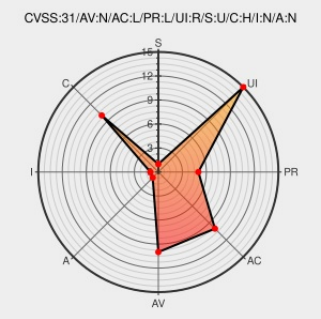
CVE-2022-47951

Published on: Not Yet Published

Last Modified on: 02/06/2023 05:27:00 PM UTC

CVE-2022-47951

Source: Mitre | Source: NIST | CVE.ORG | Print: PDF



Certain versions of Debian Linux from Debian contain the following vulnerability:

An issue was discovered in OpenStack Cinder before 19.1.2, 20.x before 20.0.2, and 21.0.0; Glance before 23.0.1, 24.x before 24.1.1, and 25.0.0; and Nova before 24.1.2, 25.x before 25.0.2, and 26.0.0. By supplying a specially created VMDK flat image that references a specific backing file path, an authenticated user may convince systems to return a copy of that file's contents from the server, resulting in unauthorized access to potentially sensitive data.

CVE-2022-47951 has been assigned by cve@mitre.org to track the vulnerability - currently rated as MEDIUM severity.

CVSS3 Score: 5.7 - MEDIUM

Attack Vector	Attack Complexity	Privileges Required	User Interaction
NETWORK	LOW	LOW	REQUIRED
Scope	**Confidentiality Impact**	**Integrity Impact**	**Availability Impact**
UNCHANGED	HIGH	NONE	NONE

CVE References

Description	Tags	Link
[SECURITY] [DLA 3300-1] glance security update	lists.debian.org text/html	MLIST [debian-lts-announce] 20230130 [SECURITY] [DLA 3300-1] glance security update
Debian -- Security Information -- DSA-5338-1 cinder	www.debian.org Depreciated Link text/html	DEBIAN DSA-5338
Bug #1996188 “[OSSA-2023-002] Arbitrary file access through cust...” : Bugs : OpenStack Compute (nova)	launchpad.net text/html	MISC launchpad.net/bugs/1996188
Debian -- Security Information -- DSA-5337-1 nova	www.debian.org	DEBIAN DSA-5337

	Depreciated Link text/html	
[SECURITY] [DLA 3302-1] nova security update	lists.debian.org text/html	MLIST [debian-lts-announce] 20230130 [SECURITY] [DLA 3302-1] nova security update
OSSA-2023-002: Arbitrary file access through custom VMDK flat descriptor — OpenStack Security Advisories 0.0.1.dev260 documentation	security.openstack.org text/html	CONFIRM security.openstack.org/ossa/OSSA-2023-002.html
Debian -- Security Information -- DSA-5336-1 glance	www.debian.org Depreciated Link text/html	DEBIAN DSA-5336
[SECURITY] [DLA 3301-1] cinder security update	lists.debian.org text/html	MLIST [debian-lts-announce] 20230130 [SECURITY] [DLA 3301-1] cinder security update

Related QID Numbers

181521 Debian Security Update for cinder (DLA 3301-1)

181528 Debian Security Update for glance (DLA 3300-1)

181529 Debian Security Update for nova (DLA 3302-1)

181536 Debian Security Update for nova (DSA 5337-1)

181537 Debian Security Update for glance (DSA 5336-1)

181538 Debian Security Update for cinder (DSA 5338-1)

199140 Ubuntu Security Notification for Nova Vulnerability (USN-5835-3)

199141 Ubuntu Security Notification for OpenStack Glance Vulnerability (USN-5835-2)

199142 Ubuntu Security Notification for Cinder Vulnerability (USN-5835-1)

199162 Ubuntu Security Notification for Nova Vulnerability (USN-5835-5)

199163 Ubuntu Security Notification for Cinder Vulnerability (USN-5835-4)

241231 Red Hat Update for OpenStack Platform 17.0 (RHSA-2023:1015)

241232 Red Hat Update for OpenStack Platform 17.0 (RHSA-2023:1016)

241235 Red Hat Update for OpenStack Platform 17.0 (RHSA-2023:1017)

241264 Red Hat Update for multiple OpenStack Platforms (RHSA-2023:1279)

241265 Red Hat Update for multiple OpenStack Platforms (RHSA-2023:1278)

241270 Red Hat Update for multiple OpenStack Platforms (RHSA-2023:1280)

Exploit/POC from Github

An issue was discovered in OpenStack Cinder before 19.1.2, 20.x before 20.0.2, and 21.0.0;

Glance before 23.0.1, 24.x…

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Debian	Debian Linux	10.0	All	All	All
Operating System	Debian	Debian Linux	11.0	All	All	All
Application	Openstack	Cinder	All	All	All	All
Application	Openstack	Cinder	All	All	All	All
Application	Openstack	Glance	All	All	All	All
Application	Openstack	Nova	All	All	All	All

cpe:2.3:o:debian:debian_linux:10.0:*:*:*:*:*:*:*:

cpe:2.3:o:debian:debian_linux:11.0:*:*:*:*:*:*:*:

cpe:2.3:a:openstack:cinder:*:*:*:*:*:*:*:*:

cpe:2.3:a:openstack:cinder:*:*:*:*:*:*:*:*:

cpe:2.3:a:openstack:glance:*:*:*:*:*:*:*:*:

cpe:2.3:a:openstack:nova:*:*:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

Social Mentions

Source	Title	Posted (UTC)
@scs_osballiance	@OVHcloud found a vulnerability (CVE-2022-47951) in the VMDK image processing code in @OpenStack Cinder, Glance and… twitter.com/i/web/status/1…	2023-01-24 16:09:36
@oss_security	[OSSA-2023-002] Cinder, Glance, Nova: Arbitrary file access through custom VMDK flat descriptor (CVE-2022-47951): P… twitter.com/i/web/status/1…	2023-01-24 17:32:04
@elburro	via feed: Sovereign Cloud Stack Security Advisory VMDK image processing (CVE-2022-47951) scs.community/security/2023/… Th… twitter.com/i/web/status/1…	2023-01-24 19:10:15
@CVEreport	cve.report/CVE-2022-47951 An issue was discovered in OpenStack Cinder before 19.1.2, 20.x before 20.0.2, and 21.0.0;… twitter.com/i/web/status/1…	2023-01-26 23:38:58
/r/netcve	CVE-2022-47951	2023-01-27 00:39:07

← Previous ID

Next ID→

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