



CVE-2017-7200

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

Summary

CVE	CVE-2017-7200
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2017-03-21 06:59:00 UTC
Updated	2017-03-30 16:39:00 UTC
Description	An SSRF issue was discovered in OpenStack Glance before Newton. The 'copy_from' feature in the Image Service API v1

Risk And Classification

Problem Types: CWE-918

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Openstack	Glance	All	All	All	All

References

Reference	Source	Link	Tags
Bug #1153614 "Add a policy to control copy-from functionality" : Bugs : Glance	CONFIRM	bugs.launchpad.net	Threat Intelligence
OSSN/OSSN-0078 - OpenStack	CONFIRM	wiki.openstack.org	Vulnerability
OpenStack Glance CVE-2017-7200 Security Bypass Vulnerability	BID	www.securityfocus.com	Threat Intelligence
Bug #1606495 "copy_from in api v1 allows network port scan" : Bugs : OpenStack Security Notes	CONFIRM	bugs.launchpad.net	Threat Intelligence
CVE Program record	CVE.ORG	www.cve.org	Canonical
NVD vulnerability detail	NVD	nvd.nist.gov	Canonical

No vendor comments have been submitted for this CVE.

There are currently no legacy QID mappings associated with this CVE.

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](#)