



CVE-2017-17051

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

Summary

CVE	CVE-2017-17051
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2017-12-05 18:29:00 UTC
Updated	2019-10-03 00:03:00 UTC
Description	An issue was discovered in the default FilterScheduler in OpenStack Nova 16.0.3. By repeatedly rebuilding an instance with

Risk And Classification

Problem Types: CWE-400

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Openstack	Nova	16.0.3	All	All	All
Application	Openstack	Nova	16.0.3	All	All	All

References

Reference

[Gerrit Code Review](#)

[Bug #1732976 "\[OSSA-2017-006\] Potential DoS by rebuilding the sa..." : Bugs : OpenStack Compute \(nova\)](#)

[OSSA-2017-006: Nova FilterScheduler doubles resource allocations during rebuild with new image — openstack-security-advisories 2014.2.0](#)

[OpenStack Nova CVE-2017-17051 Incomplete Fix Denial of Service Vulnerability](#)

[Gerrit Code Review](#)

[CVE Program record](#)

[NVD vulnerability detail](#)

No vendor comments have been submitted for this CVE.

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

© [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](#)