



CVE-2017-7555

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

Summary

CVE	CVE-2017-7555
State	PUBLIC
Assigner	secalert@redhat.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2017-08-17 19:29:00 UTC
Updated	2017-12-09 02:29:00 UTC
Description	Augeas versions up to and including 1.8.0 are vulnerable to heap-based buffer overflow due to improper handling of escape

Risk And Classification

Problem Types: CWE-119

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Augeas	Augeas	All	All	All	All

References

Reference	Source
Debian -- Security Information -- DSA-3949-1 augeas	DEBIAN
* src/pathx.c (parse_name): correctly handle trailing whitespace in n... by lutter · Pull Request #480 · hercules-team/augeas · GitHub	MISC
CVE-2017-7555 - Memory Corruption Vulnerability in augeas Puppet	CONF
Red Hat Customer Portal	REDHAT
Red Hat Customer Portal	REDHAT
augeas CVE-2017-7555 Memory Corruption Vulnerability	BID
CVE Program record	CVE.C
NVD vulnerability detail	NVD

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](#).

Free CVE JSON API [cve.report/api](#)

CVE.report and Source URL Uptime Status [status.cve.report](#)