



# CVE-2020-3123

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

## Summary

<b>CVE</b>	CVE-2020-3123
<b>State</b>	PUBLIC
<b>Assigner</b>	psirt@cisco.com
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2020-02-05 18:15:00 UTC
<b>Updated</b>	2022-01-01 19:56:00 UTC
<b>Description</b>	A vulnerability in the Data-Loss-Prevention (DLP) module in Clam AntiVirus (ClamAV) Software versions 0.102.1 and 0.102

## Risk And Classification

### Problem Types: CWE-125

## NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	<a href="#">Canonical</a>	<a href="#">Ubuntu Linux</a>	12.04	All	All	All
Operating System	<a href="#">Canonical</a>	<a href="#">Ubuntu Linux</a>	14.04	All	All	All
Operating System	<a href="#">Canonical</a>	<a href="#">Ubuntu Linux</a>	16.04	All	All	All
Operating System	<a href="#">Canonical</a>	<a href="#">Ubuntu Linux</a>	18.04	All	All	All
Operating System	<a href="#">Canonical</a>	<a href="#">Ubuntu Linux</a>	19.10	All	All	All
Application	<a href="#">Clamav</a>	<a href="#">Clamav</a>	0.102.0	All	All	All
Application	<a href="#">Clamav</a>	<a href="#">Clamav</a>	0.102.1	All	All	All
Application	<a href="#">Clamav</a>	<a href="#">Clamav</a>	0.102.0	All	All	All
Application	<a href="#">Clamav</a>	<a href="#">Clamav</a>	0.102.1	All	All	All

## References

Reference	Source	Link	Tags
ClamAV: Multiple vulnerabilities (GLSA 202003-46) — Gentoo security	GENTOO	<a href="https://security.gentoo.org">security.gentoo.org</a>	
ClamAV® blog: ClamAV 0.102.2 security patch released	CONFIRM	<a href="https://blog.clamav.net">blog.clamav.net</a>	
USN-4280-2: ClamAV vulnerability   Ubuntu security notices   Ubuntu	UBUNTU	<a href="https://usn.ubuntu.com">usn.ubuntu.com</a>	
USN-4280-1: ClamAV vulnerability   Ubuntu security notices   Ubuntu	UBUNTU	<a href="https://usn.ubuntu.com">usn.ubuntu.com</a>	
Bug Not Available	CISCO	<a href="https://quickview.cloudapps.cisco.com">quickview.cloudapps.cisco.com</a>	Third Party Advisory

CVE Program record	CVE.ORG	<a href="http://www.cve.org">www.cve.org</a>	canonical
NVD vulnerability detail	NVD	<a href="http://nvd.nist.gov">nvd.nist.gov</a>	canonical, analysis
No vendor comments have been submitted for this CVE.			
<b>Legacy QID Mappings</b>			
500097 Alpine Linux Security Update for clamav			
503822 Alpine Linux Security Update for clamav			
750483 OpenSUSE Security Update for clamav (openSUSE-SU-2020:2276-1)			
750485 OpenSUSE Security Update for clamav (openSUSE-SU-2020:2268-1)			

© [CVE.report](http://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](http://The MITRE Corporation) and the authoritative source of CVE content is [MITRE's CVE web site](http://MITRE's CVE web site). This site includes MITRE data granted under the following [license](http://license).

**CVE.report and Source URL Uptime Status [status.cve.report](http://status.cve.report)**