



CVE-2018-1000550

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

Summary

CVE	CVE-2018-1000550
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2018-06-26 16:29:00 UTC
Updated	2020-08-04 21:15:00 UTC
Description	The Sympa Community Sympa version prior to version 6.2.32 contains a Directory Traversal vulnerability in wwsympa.fcgi

Risk And Classification

Problem Types: CWE-22

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Debian	Debian Linux	8.0	All	All	All
Operating System	Debian	Debian Linux	8.0	All	All	All
Application	Sympa	Sympa	All	All	All	All
Application	Sympa	Sympa	All	All	All	All

References

Reference	Source	Link	Tags
[SECURITY] [DLA 1441-1] sympa security update	MLIST	lists.debian.org	Mailing L
USN-4442-1: Sympa vulnerabilities Ubuntu security notices Ubuntu	UBUNTU	usn.ubuntu.com	
2018-001 Security flaws in template editing - Sympa, mailing list management software	MISC	sympa-community.github.io	Patch, V
Debian -- Security Information -- DSA-4285-1 sympa	DEBIAN	www.debian.org	
CVE Program record	CVE.ORG	www.cve.org	canonica
NVD vulnerability detail	NVD	nvd.nist.gov	canonica

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](#)