



CVE-2020-29668

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

Summary

CVE	CVE-2020-29668
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2020-12-10 08:15:00 UTC
Updated	2023-11-07 03:21:00 UTC
Description	Sympa before 6.2.59b.2 allows remote attackers to obtain full SOAP API access by sending any arbitrary string (except one

Risk And Classification

Problem Types: CWE-287 | CWE-565

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Debian	Debian Linux	10.0	All	All	All
Operating System	Debian	Debian Linux	9.0	All	All	All
Operating System	Fedoraproject	Fedora	32	All	All	All
Operating System	Fedoraproject	Fedora	33	All	All	All
Application	Sympa	Sympa	6.2.59	beta1	All	All
Application	Sympa	Sympa	6.2.59	beta1	All	All
Application	Sympa	Sympa	All	All	All	All

References

Reference
sympa/NEWS.md at 6.2.59b.2 · sympa-community/sympa · GitHub
[SECURITY] Fedora 32 Update: sympa-6.2.60-1.fc32 - package-announce - Fedora Mailing-Lists
#976020 - sympa: CVE-2020-29668: Unauthorized access to review call of the SOAP API - Debian Bug report logs
Properly check email and session id in authenticateAndRun SOAP call (#1041) by racke · Pull Request #1044 · sympa-community/sympa · GitHub
[SECURITY] Fedora 33 Update: sympa-6.2.60-1.fc33 - package-announce - Fedora Mailing-Lists
[SECURITY] Fedora 33 Update: sympa-6.2.60-1.fc33 - package-announce - Fedora Mailing-Lists
[SECURITY] Fedora 32 Update: sympa-6.2.60-1.fc32 - package-announce - Fedora Mailing-Lists

[SECURITY] [DLA 2499-1] sympa security update
Unauthorised full access via SOAP API due to illegal cookie · Issue #1041 · sympa-community/sympa · GitHub
Debian -- Security Information -- DSA-4818-1 sympa
CVE Program record
NVD vulnerability detail
No vendor comments have been submitted for this CVE.
Legacy QID Mappings
690350 Free Berkeley Software Distribution (FreeBSD) Security Update for sympa (0add6e6b-6883-11eb-b0cb-f8b156c2bfe9)

© [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](#)