



CVE-2023-38686

[MITRE](#)[NVD](#)[CVE.ORG](#)[JSON API](#)[Print: PDF !\[\]\(003082e50e3009141f59bd5df831749f_img.jpg\)](#)

Summary

CVE	CVE-2023-38686
State	PUBLIC
Assigner	security-advisories@github.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2023-08-04 16:15:00 UTC
Updated	2023-08-10 19:30:00 UTC
Description	Sydent is an identity server for the Matrix communications protocol. Prior to version 2.5.6, if configured to send emails using

Risk And Classification

Problem Types: CWE-295

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Matrix	Sydent	All	All	All	All

References

Reference	Source
Explicitly create an SSL context when emailing (#574) · matrix-org/sydent@1cd7483 · GitHub	MISC
Enable TLS hostname verification by default for SMTP/IMAP/FTP/POP/NNTP protocols · Issue #91826 · python/cpython · GitHub	MISC
PEP 476 – Enabling certificate verification by default for stdlib http clients peps.python.org	MISC
Sydent does not verify email server certificates · Advisory · matrix-org/sydent · GitHub	MISC
ssl — TLS/SSL wrapper for socket objects — Python 3.9.5 documentation	MISC
Release v2.5.6 · matrix-org/sydent · GitHub	MISC
Explicitly create an SSL context when emailing by DMRobertson · Pull Request #574 · matrix-org/sydent · GitHub	MISC
CVE Program record	CVE.ORG
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](#)