



CVE-2023-27582

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

Summary

CVE	CVE-2023-27582
State	PUBLIC
Assigner	security-advisories@github.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2023-03-13 22:15:00 UTC
Updated	2023-03-17 16:20:00 UTC
Description	maddy is a composable, all-in-one mail server. Starting with version 0.2.0 and prior to version 0.6.3, maddy allows a full aut

Risk And Classification

Problem Types: CWE-287

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Maddy Project	Maddy	All	All	All	All

References

Reference	Source	Link	Tags
Full authentication bypass if SASL authorization username is specified · Advisory · foxcpp/maddy · GitHub	MISC	github.com	
Release maddy 0.6.3 · foxcpp/maddy · GitHub	MISC	github.com	
Revert authorization/authentication split · foxcpp/maddy@55a91a3 · GitHub	MISC	github.com	
auth: Actually check SASL identity argument before using it · foxcpp/maddy@9f58cb6 · GitHub	MISC	github.com	
CVE Program record	CVE.ORG	www.cve.org	canonical
NVD vulnerability detail	NVD	nvd.nist.gov	canonical

No vendor comments have been submitted for this CVE.

There are currently no legacy QID mappings associated with this CVE.

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](#)