



CVE-2023-0777

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

Summary

CVE	CVE-2023-0777
State	PUBLIC
Assigner	security@huntr.dev
Source Priority	CVE Program / NVD first with legacy fallback
Published	2023-02-10 19:15:00 UTC
Updated	2023-04-06 17:15:00 UTC
Description	Authentication Bypass by Primary Weakness in GitHub repository modoboa/modoboa prior to 2.0.4.

Risk And Classification

Problem Types: CWE-305

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Modoboa	Modoboa	All	All	All	All

References

Reference	Source	Link	Ta
modoboa 2.0.4 Admin Takeover ≈ Packet Storm	MISC	packetstormsecurity.com	
huntr – Security Bounties for any GitHub repository	CONFIRM	huntr.dev	
Merge pull request #2767 from modoboa/api-throttling · modoboa/modoboa@47d17ac · GitHub	MISC	github.com	
CVE Program record	CVE.ORG	www.cve.org	ca
NVD vulnerability detail	NVD	nvd.nist.gov	ca

No vendor comments have been submitted for this CVE.

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

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