



CVE-2020-5233

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

Summary

CVE	CVE-2020-5233
State	PUBLIC
Assigner	security-advisories@github.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2020-01-30 19:15:00 UTC
Updated	2020-04-09 14:33:00 UTC
Description	OAuth2 Proxy before 5.0 has an open redirect vulnerability. Authentication tokens could be silently harvested by an attacker

Risk And Classification

Problem Types: CWE-601

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Oauth2 Proxy Project	Oauth2 Proxy	All	All	All	All
Application	Oauth2 Proxy Project	Oauth2 Proxy	All	All	All	All

References

Reference	Source
Merge pull request from GHSA-qqxw-m5fj-f7gv · oauth2-proxy/oauth2-proxy@a316f8a · GitHub	MITRE
Release v5.0.0 · oauth2-proxy/oauth2-proxy · GitHub	MITRE
The pattern '/\domain.com' is not disallowed when redirecting, allowing for open redirect · Advisory · oauth2-proxy/oauth2-proxy · GitHub	CC
CVE Program record	CV
NVD vulnerability detail	NV

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