



CVE-2021-31606

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

Summary

CVE	CVE-2021-31606
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2021-09-27 06:15:00 UTC
Updated	2023-12-22 15:15:00 UTC
Description	furlongm openvpn-monitor through 1.1.3 allows Authorization Bypass to disconnect arbitrary clients.

Risk And Classification

Problem Types: CWE-287

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Openvpn-monitor Project	Openvpn-monitor	All	All	All	All

References

Reference	Source	Link	Tags
OpenVPN Monitor 1.1.3 Authorization Bypass / Denial Of Service ≈ Packet Storm	MISC	packetstormsecurity.com	
github.com/furlongm/openvpn-monitor/commit/ddb9d31ef0ec56f578bdacf99ebe9...		github.com	
Releases · furlongm/openvpn-monitor · GitHub	MISC	github.com	
CVE Program record	CVE.ORG	www.cve.org	canonical
NVD vulnerability detail	NVD	nvd.nist.gov	canonical, anal

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

[997503](#) Python (Pip) Security Update for openvpn-monitor (GHSA-5w5c-3g26-8mmc)

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