



CVE-2019-12105

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

Summary

CVE	CVE-2019-12105
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2019-09-10 17:15:00 UTC
Updated	2023-11-07 03:03:00 UTC
Description	** DISPUTED ** In Supervisor through 4.0.2, an unauthenticated user can read log files or restart a service. Note: The main

Risk And Classification

Problem Types: CWE-306

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Supervisord	Supervisor	All	All	All	All

References

Reference	Source	Link
Add an explicit security warning about inet_http_server. · Supervisor/supervisor@4e334d9 · GitHub	MISC	g
Configuration File — Supervisor 4.2.2 documentation	MISC	s
[CVE-2019-12105] Unauthenticated user can read log files or restart a service · Issue #1245 · Supervisor/supervisor · GitHub	MISC	g
CVE Program record	CVE.ORG	v
NVD vulnerability detail	NVD	r

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

[500680](#) Alpine Linux Security Update for supervisor

[504449](#) Alpine Linux Security Update for supervisor

© [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](#)