



CVE-2022-46768

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

Summary

CVE	CVE-2022-46768
State	PUBLIC
Assigner	security@zabbix.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2022-12-15 07:15:00 UTC
Updated	2022-12-19 15:23:00 UTC
Description	Arbitrary file read vulnerability exists in Zabbix Web Service Report Generation, which listens on the port 10053. The service

Risk And Classification

Problem Types: CWE-20

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Zabbix	Web Service Report Generation	All	All	All	All
Application	Zabbix	Web Service Report Generation	All	All	All	All
Application	Zabbix	Zabbix-agent2	All	All	All	All

References

Reference

[ZBX-22087] Zabbix Web Service Report Generation External Control of File Name Information Disclosure Vulnerability (CVE-2022-46768) - Z

CVE Program record

NVD vulnerability detail

Vendor Comments And Credit

Discovery Credit

LEGACY: Trend Micro ZDI

Legacy QID Mappings

[182229](#) Debian Security Update for zabbix (CVE-2022-46768)

© [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](#)