



CVE-2023-32724

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

Summary

CVE	CVE-2023-32724
State	PUBLIC
Assigner	security@zabbix.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2023-10-12 07:15:00 UTC
Updated	2023-10-17 15:08:00 UTC
Description	Memory pointer is in a property of the Ducktape object. This leads to multiple vulnerabilities related to direct memory access:

Risk And Classification

Problem Types: CWE-732

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Zabbix	Zabbix	7.0.0	alpha1	All	All
Application	Zabbix	Zabbix	7.0.0	alpha2	All	All
Application	Zabbix	Zabbix	7.0.0	alpha3	All	All
Application	Zabbix	Zabbix	All	All	All	All
Application	Zabbix	Zabbix	All	All	All	All
Application	Zabbix	Zabbix	All	All	All	All

References

Reference	Source
[ZBX-23391] JS engine memory pointers are directly available for Zabbix users for modification (CVE-2023-32724) - ZABBIX SUPPORT	MI
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.

© [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](#)