



CVE-2022-43515

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

Summary

CVE	CVE-2022-43515
State	PUBLIC
Assigner	security@zabbix.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2022-12-05 19:15:00 UTC
Updated	2023-08-22 19:16:00 UTC
Description	Zabbix Frontend provides a feature that allows admins to maintain the installation and ensure that only certain IP addresses

Risk And Classification

Problem Types: CWE-863

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Zabbix	Frontend	5.0.30	rc1	All	All
Application	Zabbix	Frontend	6.0.11	rc1	All	All
Application	Zabbix	Frontend	6.2.5	rc1	All	All
Application	Zabbix	Frontend	All	All	All	All
Application	Zabbix	Frontend	All	All	All	All
Application	Zabbix	Frontend	All	All	All	All
Application	Zabbix	Frontend	All	All	All	All

References

Reference
[SECURITY] [DLA 3538-1] zabbix security update
[ZBX-22050] X-Forwarded-For header is active by default causes access to zabbix sites in maintenance mode (CVE-2022-43515) - ZABBIX S
Log in - ZABBIX SUPPORT
CVE Program record
NVD vulnerability detail

Vendor Comments And Credit

Discovery Credit

LEGACY: osman1337

Legacy QID Mappings

6000015 Debian Security Update for zabbix (DLA 3538-1)

753005 SUSE Enterprise Linux Security Update for zabbix (SUSE-SU-2022:4477-1)

© [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](#).

CVE.report and Source URL Uptime Status [status.cve.report](#)