



CVE-2022-28173

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

Summary

CVE	CVE-2022-28173
State	PUBLIC
Assigner	hsrc@hikvision.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2022-12-19 16:15:00 UTC
Updated	2022-12-29 18:46:00 UTC
Description	The web server of some Hikvision wireless bridge products have an access control vulnerability which can be used to obtain

Risk And Classification

Problem Types: NVD-CWE-Other

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Hardware	Hikvision	Ds-3wf01c-2n/o	-	All	All	All
Operating System	Hikvision	Ds-3wf01c-2n/o Firmware	All	All	All	All
Hardware	Hikvision	Ds-3wf0ac-2nt	-	All	All	All
Operating System	Hikvision	Ds-3wf0ac-2nt Firmware	All	All	All	All

References

Reference	Source
Security Notification - Access Control Vulnerability in Some Hikvision Wireless Bridge Products - Security Advisory - Hikvision	MISC
CVE Program record	CVE.ORG
NVD vulnerability detail	NVD

Vendor Comments And Credit

Discovery Credit

LEGACY: Souvik Kandar, Arko Dhar

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](#)