



CVE-2023-0956

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

Summary

CVE	CVE-2023-0956
State	PUBLIC
Assigner	ics-cert@hq.dhs.gov
Source Priority	CVE Program / NVD first with legacy fallback
Published	2023-08-03 19:15:00 UTC
Updated	2023-08-08 20:10:00 UTC
Description	External input could be used on TEL-STER TelWin SCADA WebInterface to construct paths to files and directories without

Risk And Classification

Problem Types: CWE-22

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Tel-ster	Telwin Scada Webinterface	All	All	All	All
Application	Tel-ster	Telwin Scada Webinterface	8.0	All	All	All
Application	Tel-ster	Telwin Scada Webinterface	9.0	All	All	All

References

Reference
Nie znalezione strony CERT Polska
TEL-STER Sp. z o.o. System SCADA Oprogramowanie Automatyka Wizualizacja Nominacje - Ważne! Krytyczna podatność TelWin SC
TEL-STER TelWin SCADA WebInterface CISA
CVE Program record
NVD vulnerability detail

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](#)