



CVE-2020-16199

[MITRE](#)[NVD](#)[CVE.ORG](#)[Print: PDF !\[\]\(e3f8612927870f2e0f9f5989e6dd3064_img.jpg\)](#)

Summary

CVE	CVE-2020-16199
State	PUBLIC
Assigner	ics-cert@hq.dhs.gov
Source Priority	CVE Program / NVD first with legacy fallback
Published	2020-08-04 19:15:00 UTC
Updated	2020-08-06 18:18:00 UTC
Description	Delta Industrial Automation CNCSoft ScreenEditor, Versions 1.01.23 and prior. Multiple stack-based buffer overflow vulnerera

Risk And Classification

Problem Types: CWE-787

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Deltaww	Cncsoft Screeneditor	All	All	All	All

References

Reference	Source	Link	Tags
ZDI-20-943 Zero Day Initiative	MISC	www.zerodayinitiative.com	Third Party Advisory, VDB Entry
Delta Industrial Automation CNCSoft ScreenEditor CISA	MISC	us-cert.cisa.gov	Third Party Advisory, US Government I
ZDI-20-939 Zero Day Initiative	MISC	www.zerodayinitiative.com	Third Party Advisory, VDB Entry
ZDI-20-940 Zero Day Initiative	MISC	www.zerodayinitiative.com	Third Party Advisory, VDB Entry
CVE Program record	CVE.ORG	www.cve.org	canonical
NVD vulnerability detail	NVD	nvd.nist.gov	canonical, analysis

No vendor comments have been submitted for this CVE.

There are currently no legacy QID mappings associated with this CVE.

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](#)