



CVE-2018-8840

[MITRE](#)[NVD](#)[CVE.ORG](#)[JSON API](#)[Print: PDF !\[\]\(003082e50e3009141f59bd5df831749f_img.jpg\)](#)

Summary

CVE	CVE-2018-8840
State	PUBLIC
Assigner	ics-cert@hq.dhs.gov
Source Priority	CVE Program / NVD first with legacy fallback
Published	2018-04-18 20:29:00 UTC
Updated	2019-10-09 23:42:00 UTC
Description	A remote attacker could send a carefully crafted packet in InduSoft Web Studio v8.1 and prior versions, and/or InTouch Ma

Risk And Classification

Problem Types: CWE-119

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Indusoft	Web Studio	All	All	All	All
Application	Industrial-software	Intouch Machine Edition 2017	All	All	All	All

References

Reference	Source
[R2] Schneider Electric InduSoft Web Studio and InTouch Machine Edition Remote Code Execution - Research Advisory Tenable™	MISC
Schneider Electric InduSoft Web Studio and InTouch Machine Edition ICS-CERT	MISC
AVEVA - Global Leader in Industrial Software	MISC
Malformed Request	BID
CVE Program record	CVE.C
NVD vulnerability detail	NVD

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](#)