



CVE-2017-9641

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

Summary

CVE	CVE-2017-9641
State	PUBLIC
Assigner	ics-cert@hq.dhs.gov
Source Priority	CVE Program / NVD first with legacy fallback
Published	2018-05-25 15:29:00 UTC
Updated	2019-10-09 23:30:00 UTC
Description	PI Coresight 2016 R2 contains a cross-site request forgery vulnerability that may allow access to the PI system. OSISOFT rec

Risk And Classification

Problem Types: CWE-352

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Osisoft	Pi Coresight	All	All	All	All

References

Reference	Source	Link	Tags
OSISOFT PI Coresight ICS-CERT	MISC	ics-cert.us-cert.gov	Third Party Advisory
OSISOFT PI Coresight CVE-2017-9641 Cross Site Request Forgery Vulnerability	BID	www.securityfocus.com	Third Party Advisory
OSISOFT releases security updates for PI Coresight with PI Vision 2017	CONFIRM	techsupport.osisoft.com	Vendor Advisory
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.

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