CVE-2016-7960

MITRE | NVD | CVE.ORG | JSON API | Print: PDF

Summary

CVE	CVE-2016-7960
State	PUBLISHED
Assigner	mitre
Source Priority	CVE Program / NVD first with legacy fallback
Published	2016-10-13 10:59:01 UTC
Updated	2026-05-06 22:30:45 UTC
Description	Siemens SIMATIC STEP 7 (TIA Portal) before 14 uses an improper format for managing TIA project files during version up

Risk And Classification

Primary CVSS: v3.0 2.5 LOW from nvd@nist.gov

CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:L/I:N/A:N

EPSS: 0.000880000 probability, percentile 0.248770000 (date 2026-05-07)

Problem Types: CWE-200 | n/a

Version	Source	Type	Score	Severity	Vector
3.0	nvd@nist.gov	Primary	2.5	LOW	CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:L/I:N/A:N
2.0	nvd@nist.gov	Primary	1.9		AV:L/AC:M/Au:N/C:P/I:N/A:N

CVSS v3.0 Breakdown

Attack Vector

Local

Attack Complexity

High

Privileges Required

Low

User Interaction

None

Scope

Unchanged

Confidentiality

Low

Integrity

None

Availability

None

CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:L/I:N/A:N

CVSS v2.0 Breakdown

Access Vector

Local

Access Complexity

Medium

Authentication

None

Confidentiality

Partial

Integrity

None

Availability

None

AV:L/AC:M/Au:N/C:P/I:N/A:N

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Siemens	Simatic Step 7	All	All	All	All

Vendor Declared Affected Products

Source	Vendor	Product	Version	Platforms
CNA	Na	N/a	affected n/a	Not specified

References

Reference	Source	Link
Siemens	af854a3a-2127-422b-91ae-364da2661108	www
SIMATIC STEP 7 (TIA Portal) Multiple Local Information Disclosure Vulnerabilities	af854a3a-2127-422b-91ae-364da2661108	www
Siemens SIMATIC STEP 7 (TIA Portal) Information Disclosure Vulnerabilities | ICS-CERT	af854a3a-2127-422b-91ae-364da2661108	ics-c
CVE Program record	CVE.ORG	www
NVD vulnerability detail	NVD	nvd.

No vendor comments have been submitted for this CVE.

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

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

Free CVE JSON API cve.report/api

CVE.report and Source URL Uptime Status **status.cve.report**