



# CVE-2017-14029

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

## Summary

<b>CVE</b>	CVE-2017-14029
<b>State</b>	PUBLISHED
<b>Assigner</b>	icscert
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2017-11-06 22:29:00 UTC
<b>Updated</b>	2025-04-20 01:37:25 UTC
<b>Description</b>	An Uncontrolled Search Path Element issue was discovered in Trihedral VTScada 11.3.03 and prior. The program will exec

## Risk And Classification

**Primary CVSS:** v3.0 7.8 HIGH from nvd@nist.gov

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

**Problem Types:** CWE-427 | CWE-427 CWE-427

Version	Source	Type	Score	Severity	Vector
3.0	nvd@nist.gov	Primary	7.8	HIGH	<b>CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H</b>
2.0	nvd@nist.gov	Primary	9.3		<b>AV:N/AC:M/Au:N/C:C/I:C/A:C</b>

## CVSS v3.0 Breakdown

Attack Vector

Local

Attack Complexity

Low

Privileges Required

None

User Interaction

Required

Scope

Unchanged

Confidentiality

High

Integrity

High

Availability

High

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

### CVSS v2.0 Breakdown

Access Vector

Network

Access Complexity

Medium

Authentication

None

Confidentiality

Complete

Integrity

Complete

Availability

Complete

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

### NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Trihedral	Vtscada	All	All	All	All

### Vendor Declared Affected Products

Source	Vendor	Product	Version	Platforms
CNA	Na	Trihedral Engineering Limited VTScada	affected Trihedral Engineering Limited VTScada	Not specified

### References

Reference	Source	Link	Tags
Trihedral Engineering Limited VTScada   CISA	af854a3a-2127-422b-91ae-364da2661108	<a href="https://ics-cert.us-cert.gov">ics-cert.us-cert.gov</a>	Issue Tracking, Mitigation
CVE Program record	CVE.ORG	<a href="https://www.cve.org">www.cve.org</a>	canonical
NVD vulnerability detail	NVD	<a href="https://nvd.nist.gov">nvd.nist.gov</a>	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](#).

**Free CVE JSON API** [cve.report/api](https://cve.report/api)

**CVE.report and Source URL Uptime Status** [status.cve.report](https://status.cve.report)