



# CVE-2016-2281

[MITRE](#)[NVD](#)[CVE.ORG](#)[JSON API](#)[Print: PDF !\[\]\(003082e50e3009141f59bd5df831749f\_img.jpg\)](#)

## Summary

<b>CVE</b>	CVE-2016-2281
<b>State</b>	PUBLISHED
<b>Assigner</b>	icscert
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2016-03-18 14:59:04 UTC
<b>Updated</b>	2026-05-06 22:30:45 UTC
<b>Description</b>	Untrusted search path vulnerability in ABB Panel Builder 800 5.1 allows local users to gain privileges via a Trojan horse DL

## Risk And Classification

**Primary CVSS:** v3.0 7.2 HIGH from nvd@nist.gov

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

**Problem Types:** CWE-264 | n/a

Version	Source	Type	Score	Severity	Vector
3.0	nvd@nist.gov	Primary	7.2	HIGH	<b>CVSS:3.0/AV:L/AC:H/PR:H/UI:R/S:C/C:H/I:H/A:H</b>
2.0	nvd@nist.gov	Primary	6		<b>AV:L/AC:H/Au:S/C:C/I:C/A:C</b>

## CVSS v3.0 Breakdown

Attack Vector

Local

Attack Complexity

High

Privileges Required

High

User Interaction

Required

Scope

Changed

Confidentiality

High

Integrity

High

Availability

High

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

### CVSS v2.0 Breakdown

Access Vector

Local

Access Complexity

High

Authentication

Single

Confidentiality

Complete

Integrity

Complete

Availability

Complete

AV:L/AC:H/Au:S/C:C/I:C/A:C

### NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Abb	Panel Builder 800	5.1	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
ABB Panel Builder 800 DLL Hijacking Vulnerability (Update A)   ICS-CERT	af854a3a-2127-422b-91ae-364da2661108	<a href="https://ics-cert.us-cert.gov">ics-cert.us-cert.gov</a>
CVE Program record	CVE.ORG	<a href="https://www.cve.org">www.cve.org</a>
NVD vulnerability detail	NVD	<a href="https://nvd.nist.gov">nvd.nist.gov</a>

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)