



# CVE-2024-56181

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

## Summary

<b>CVE</b>	CVE-2024-56181
<b>State</b>	PUBLISHED
<b>Assigner</b>	siemens
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2025-03-11 10:15:15 UTC
<b>Updated</b>	2026-04-14 09:16:34 UTC
<b>Description</b>	A vulnerability has been identified in SIMATIC Field PG M5 (All versions), SIMATIC IPC BX-21A (All versions < V31.01.07).

## Risk And Classification

**Primary CVSS:** v4.0 8.4 HIGH from productcert@siemens.com

CVSS:4.0/AV:L/AC:L/AT:N/PR:H/UI:N/VC:N/VI:H/VA:H/SC:H/SI:H/SA:H/E:X/CR:X/IR:X/AR:X/MAV:X/MAC:X/MAT:X/MPR:X/MUI:X/MVC:X/MVI:X/MVA:X/MSX/MSI:X/MSA:X/S:X/AU:X/R:X/V:X/RE:X/U:X

**EPSS:** 0.000120000 probability, percentile 0.018310000 (date 2026-04-15)

**Problem Types:** CWE-693 | CWE-693 CWE-693: Protection Mechanism Failure

Version	Source	Type	Score	Severity	Vector
4.0	productcert@siemens.com	Secondary	8.4	HIGH	CVSS:4.0/AV:L/AC:L/AT:N/PR:H/UI:N/VC:N/VI:H/VA:H/SC:H/SI:H/S
4.0	CNA	DECLARED	8.4	HIGH	CVSS:4.0/AV:L/AC:L/AT:N/PR:H/UI:N/VC:N/VI:H/VA:H/SC:H/SI:H/S
3.1	productcert@siemens.com	Secondary	8.2	HIGH	CVSS:3.1/AV:L/AC:L/PR:H/UI:N/S:C/H/I:H/A:H
3.1	CNA	DECLARED	8.2	HIGH	CVSS:3.1/AV:L/AC:L/PR:H/UI:N/S:C/H/I:H/A:H

## CVSS v4.0 Breakdown

Attack Vector

Local

Attack Complexity

Low

Attack Requirements

None

Privileges Required

High

User Interaction

None

Confidentiality

None

Integrity

High

Availability

High

Sub Conf.

High

Sub Integrity

High

Sub Availability

High

CVSS:4.0/AV:L/AC:L/AT:N/PR:H/UI:N/VC:N/VI:H/VA:H/SC:H/SI:H/SA:H/E:X/CR:X/IR:X/AR:X/MAV:X/MAC:X/MAT:X/MPR:X/MUI:X/MVC:X/MVI:X/MVA:X/MSX/MSI:X/MSA:X/S:X/AU:X/R:X/V:X/RE:X/U:X

### CVSS v3.1 Breakdown

Attack Vector

Local

Attack Complexity

Low

Privileges Required

High

User Interaction

None

Scope

Changed

Confidentiality

High

Integrity

High

Availability

High

CVSS:3.1/AV:L/AC:L/PR:H/UI:N/S:C/C:H/I:H/A:H

### Vendor Declared Affected Products

Source	Vendor	Product	Version	Platforms
CNA	Siemens	SIMATIC Field PG M5	affected * custom	Not specified
CNA	Siemens	SIMATIC IPC BX-21A	affected V31.01.07 custom	Not specified
CNA	Siemens	SIMATIC IPC BX-32A	affected V29.01.07 custom	Not specified
CNA	Siemens	SIMATIC IPC BX-39A	affected V29.01.07 custom	Not specified

CNA	Siemens	SIMATIC IPC BX-59A	affected V32.01.04 custom	Not specified
CNA	Siemens	SIMATIC IPC PX-32A	affected V29.01.07 custom	Not specified
CNA	Siemens	SIMATIC IPC PX-39A	affected V29.01.07 custom	Not specified
CNA	Siemens	SIMATIC IPC PX-39A PRO	affected V29.01.07 custom	Not specified
CNA	Siemens	SIMATIC IPC RC-543A	affected * custom	Not specified
CNA	Siemens	SIMATIC IPC RC-543B	affected V35.01.12 custom	Not specified
CNA	Siemens	SIMATIC IPC RW-543A	affected V1.1.4 custom	Not specified
CNA	Siemens	SIMATIC IPC RW-543B	affected V35.02.10 custom	Not specified
CNA	Siemens	SIMATIC IPC127E	affected V27.01.11 custom	Not specified
CNA	Siemens	SIMATIC IPC227E	affected * custom	Not specified
CNA	Siemens	SIMATIC IPC227G	affected V28.01.14 custom	Not specified
CNA	Siemens	SIMATIC IPC277E	affected * custom	Not specified
CNA	Siemens	SIMATIC IPC277G	affected V28.01.14 custom	Not specified
CNA	Siemens	SIMATICIPC277G PRO	affected V28.01.14 custom	Not specified
CNA	Siemens	SIMATIC IPC3000 SMART V3	affected * custom	Not specified
CNA	Siemens	SIMATIC IPC327G	affected V28.01.14 custom	Not specified
CNA	Siemens	SIMATIC IPC347G	affected * custom	Not specified
CNA	Siemens	SIMATIC IPC377G	affected V28.01.14 custom	Not specified
CNA	Siemens	SIMATIC IPC427E	affected * custom	Not specified
CNA	Siemens	SIMATIC IPC477E	affected * custom	Not specified
CNA	Siemens	SIMATIC IPC477E PRO	affected * custom	Not specified
CNA	Siemens	SIMATIC IPC527G	affected * custom	Not specified
CNA	Siemens	SIMATIC IPC627E	affected V25.02.15 custom	Not specified
CNA	Siemens	SIMATIC IPC647E	affected V25.02.15 custom	Not specified
CNA	Siemens	SIMATIC IPC677E	affected V25.02.15 custom	Not specified
CNA	Siemens	SIMATIC IPC847E	affected V25.02.15 custom	Not specified
CNA	Siemens	SIMATIC ITP1000	affected * custom	Not specified

## References

Reference	Source	Link	Tags
cert-portal.siemens.com/productcert/html/ssa-216014.html	productcert@siemens.com	<a href="https://cert-portal.siemens.com">cert-portal.siemens.com</a>	
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.

© [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](#)