Denial of Service Vulnerabilities in System 800xA, Symphony® Plus IEC 61850

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

Summary

CVE	CVE-2025-3756
State	PUBLISHED
Assigner	ABB
Source Priority	CVE Program / NVD first with legacy fallback
Published	2026-04-13 18:16:27 UTC
Updated	2026-04-17 15:18:16 UTC
Description	A vulnerability exists in the command handling of the IEC 61850 communication stack included in the product revisions liste

Risk And Classification

Primary CVSS: v4.0 7.1 HIGH from cybersecurity@ch.abb.com

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

EPSS: 0.000250000 probability, percentile 0.066280000 (date 2026-04-20)

Problem Types: CWE-1284 | CWE-1284 CWE-1284 Improper validation of specified quantity in input

Version	Source	Type	Score	Severity	Vector
4.0	cybersecurity@ch.abb.com	Secondary	7.1	HIGH	CVSS:4.0/AV:A/AC:L/AT:N/PR:N/UI:N/VC:N/VI:N/VA:H/SC:N/SI:N/SA
4.0	CNA	CVSS	7.1	HIGH	CVSS:4.0/AV:A/AC:L/AT:N/PR:N/UI:N/VC:N/VI:N/VA:H/SC:N/SI:N/SA
3.1	cybersecurity@ch.abb.com	Secondary	6.5	MEDIUM	CVSS:3.1/AV:A/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H
3.1	CNA	CVSS	6.5	MEDIUM	CVSS:3.1/AV:A/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H

CVSS v4.0 Breakdown

Attack Vector

Adjacent

Attack Complexity

Low

Attack Requirements

None

Privileges Required

None

User Interaction

None

Confidentiality

None

Integrity

None

Availability

High

Sub Conf.

None

Sub Integrity

None

Sub Availability

None

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

CVSS v3.1 Breakdown

Attack Vector

Adjacent

Attack Complexity

Low

Privileges Required

None

User Interaction

None

Scope

Unchanged

Confidentiality

None

Integrity

None

Availability

High

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

Vendor Declared Affected Products

Source	Vendor	Product	Version	Platforms
CNA	ABB	AC800M System 800xA	affected 6.0.0x 6.0.0303.0 custom	Not specified
CNA	ABB	AC800M System 800xA	affected 6.1.0x 6.1.0031.0 custom	Not specified

CNA	ABB	AC800M System 800xA	affected 6.1.1x 6.1.1004.0 custom	Not specified
CNA	ABB	AC800M System 800xA	affected 6.1.1x 6.1.1202.0 custom	Not specified
CNA	ABB	AC800M System 800xA	affected 6.2.0x 6.2.0006.0 custom	Not specified
CNA	ABB	Symphony Plus SD Series	affected A_0 custom	Not specified
CNA	ABB	Symphony Plus SD Series	affected A_1 custom	Not specified
CNA	ABB	Symphony Plus SD Series	affected A_2.003 custom	Not specified
CNA	ABB	Symphony Plus SD Series	affected A_3.005 custom	Not specified
CNA	ABB	Symphony Plus SD Series	affected A_4.001 custom	Not specified
CNA	ABB	Symphony Plus SD Series	affected B_0.005 custom	Not specified
CNA	ABB	Symphony Plus MR Melody Rack	affected 3.10 3.52 custom	Not specified
CNA	ABB	S Operations	affected 2.1 custom	Not specified
CNA	ABB	S Operations	affected 2.2 custom	Not specified
CNA	ABB	S Operations	affected 2.3 custom	Not specified
CNA	ABB	S Operations	affected 3.3 custom	Not specified

References

Reference	Source	Link	Tags
search.abb.com/library/Download.aspx	cybersecurity@ch.abb.com	search.abb.com	
CVE Program record	CVE.ORG	www.cve.org	canonical
NVD vulnerability detail	NVD	nvd.nist.gov	canonical, analysis

Vendor Comments And Credit

Discovery Credit

CNA: ABB thanks Hitachi Energy for sharing the information affecting a commonly used software component. (en)

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