CVE-2015-6460

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

Summary

CVE	CVE-2015-6460
State	PUBLISHED
Assigner	icscert
Source Priority	CVE Program / NVD first with legacy fallback
Published	2015-09-18 22:59:08 UTC
Updated	2026-05-06 22:30:45 UTC
Description	Multiple heap-based buffer overflows in 3S-Smart CODESYS Gateway Server before 2.3.9.34 allow remote attackers to ex

Risk And Classification

Primary CVSS: v2.0 7.5 from nvd@nist.gov

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

Problem Types: CWE-119 | n/a

CVSS v2.0 Breakdown

Access Vector

Network

Access Complexity

Low

Authentication

None

Confidentiality

Partial

Integrity

Partial

Availability

Partial

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

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	3s-smart	Codesys Gateway Server	All	All	All	All

Vendor Declared Affected Products

Source	Vendor	Product	Version	Platforms
CNA	CODESYS	3S-Smart CODESYS Gateway Server	affected V2 2.3.9.34 custom	Not specified

References

Reference	Source	Link
Zero Day Initiative	af854a3a-2127-422b-91ae-364da2661108	zerodayinitiative.com
3S CODESYS Gateway Server Buffer Overflow Vulnerability | ICS-CERT	af854a3a-2127-422b-91ae-364da2661108	ics-cert.us-cert.gov
Zero Day Initiative	af854a3a-2127-422b-91ae-364da2661108	zerodayinitiative.com
CVE Program record	CVE.ORG	www.cve.org
NVD vulnerability detail	NVD	nvd.nist.gov

No vendor comments have been submitted for this CVE.

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