CVE-2016-8378

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

Summary

CVE	CVE-2016-8378
State	PUBLISHED
Assigner	icscert
Source Priority	CVE Program / NVD first with legacy fallback
Published	2017-02-13 21:59:01 UTC
Updated	2025-04-20 01:37:25 UTC
Description	An issue was discovered in Lynxspring JENEsys BAS Bridge versions 1.1.8 and older. The application's database lacks suf

Risk And Classification

Primary CVSS: v3.0 9.8 CRITICAL from nvd@nist.gov

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

Problem Types: CWE-255 | Lynxspring JENEsys BAS Bridge lacks sufficient safeguards

Version	Source	Type	Score	Severity	Vector
3.0	nvd@nist.gov	Primary	9.8	CRITICAL	CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H
2.0	nvd@nist.gov	Primary	5		AV:N/AC:L/Au:N/C:P/I:N/A:N

CVSS v3.0 Breakdown

Attack Vector
Network

Attack Complexity
Low

Privileges Required
None

User Interaction
None

Scope
Unchanged

Confidentiality
High

Integrity
High

Availability

High

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

CVSS v2.0 Breakdown

Access Vector

Network

Access Complexity

Low

Authentication

None

Confidentiality

Partial

Integrity

None

Availability

None

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

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Lynxspring	Jenesys Bas Bridge	All	All	All	All

Vendor Declared Affected Products

Source	Vendor	Product	Version	Platform
CNA	Na	Lynxspring JENEsys BAS Bridge 1.1.8 And Older	affected Lynxspring JENEsys BAS Bridge 1.1.8 and older	Not spec

References

Reference	Source	Link
Lynxspring JENEsys BAS Bridge Vulnerabilities | ICS-CERT	af854a3a-2127-422b-91ae-364da2661108	ics-cert.us-c
Lynxspring JENEsys BAS Bridge ICSA-16-320-01 Multiple Security Vulnerabilities	af854a3a-2127-422b-91ae-364da2661108	www.securi
CVE Program record	CVE.ORG	www.cve.or
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.

Free CVE JSON API cve.report/api

CVE.report and Source URL Uptime Status status.cve.report