CVE-2012-0245

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

Summary

CVE	CVE-2012-0245
State	PUBLISHED
Assigner	certcc
Source Priority	CVE Program / NVD first with legacy fallback
Published	2012-03-09 11:55:00 UTC
Updated	2026-04-29 01:13:23 UTC
Description	Multiple stack-based buffer overflows in RobNetScanHost.exe in ABB Robot Communications Runtime before 5.14.02, as u

Risk And Classification

Primary CVSS: v2.0 10 from nvd@nist.gov

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

Problem Types: CWE-119 | n/a

CVSS v2.0 Breakdown

Access Vector

Network

Access Complexity

Low

Authentication

None

Confidentiality

Complete

Integrity

Complete

Availability

Complete

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

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Abb	Interlink Module	-	All	All	All

Application	Abb	Irc5 Opc Server	-	All	All	All
Application	Abb	Pc Sdk	-	All	All	All
Application	Abb	Pickmaster 3	-	All	All	All
Application	Abb	Pickmaster 5	-	All	All	All
Application	Abb	Robotstudio	-	All	All	All
Application	Abb	Robot Communications Runtime	All	All	All	All
Application	Abb	Robview 5	-	All	All	All
Application	Abb	Webware Sdk	-	All	All	All
Application	Abb	Webware Server	-	All	All	All

Vendor Declared Affected Products

Source	Vendor	Product	Version	Platforms
CNA	Na	N/a	affected n/a	Not specified

References

Reference	Source
ABB WebWare Server 'RobNetScanHost.exe' Buffer Overflow Vulnerability	af854a3a-2127-422b-91a
Security Advisory SA48090 - ABB Multiple Products RobNetScanHost.exe Buffer Overflow Vulnerability - Secunia	af854a3a-2127-422b-91a
404 - File Not Found | CISA	af854a3a-2127-422b-91a
Zero Day Initiative	af854a3a-2127-422b-91a
www05.abb.com/global/scot/scot348.nsf/veritydisplay/f261be074480dc24c12579a...	af854a3a-2127-422b-91a
archives.neohapsis.com/archives/bugtraq/2012-02/0125.html	af854a3a-2127-422b-91a
Not Found	MITRE
CVE Program record	CVE.ORG
NVD vulnerability detail	NVD

No vendor comments have been submitted for this CVE.

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

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