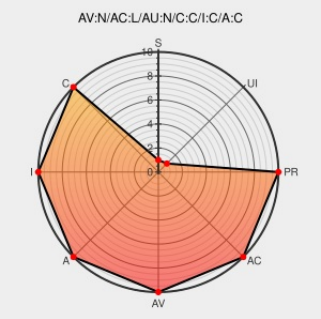
CVE-2011-5007

Published on: 12/24/2011 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:23:17 PM UTC

CVE-2011-5007

Source: Mitre | Source: NIST | CVE.ORG | Print: PDF



Certain versions of Codesys from 3ssoftware contain the following vulnerability:

Stack-based buffer overflow in the CmpWebServer component in 3S CoDeSys 3.4 SP4 Patch 2 and earlier, as used on the ABB AC500 PLC and possibly other products, allows remote attackers to execute arbitrary code via a long URI to TCP port 8080.

CVE-2011-5007 has been assigned by cve@mitre.org to track the vulnerability

CVSS2 Score: 10 - HIGH

Access Vector	Access Complexity	Authentication
NETWORK	LOW	NONE
Confidentiality Impact	**Integrity Impact**	**Availability Impact**
COMPLETE	COMPLETE	COMPLETE

CVE References

Description	Tags	Link
	aluigi.altervista.org text/plain	MISC aluigi.altervista.org/adv/codesys_1-adv.txt
CoDeSys SCADA v2.3 Remote Exploit	Exploit www.exploit-db.com Proof of Concept text/html	EXPLOIT-DB 18187
ABB AC500 PLC Webserver CoDeSys Vulnerability | ICS-CERT	ics-cert.us-cert.gov text/html	MISC ics-cert.us-cert.gov/advisories/ICSA-12-320-01
404 - File Not Found | CISA	US Government Resource www.us-cert.gov application/pdf Inactive Link Not Archived	MISC www.us-cert.gov/control_systems/pdf/ICS-ALERT-11-336-01A.pdf
404 - File Not Found | CISA	US Government Resource	MISC www.us-cert.gov/control_systems/pdf/ICS-

	www.us-cert.gov application/pdf Inactive Link Not Archived	ALERT-11-336-01.pdf
About Secunia Research | Flexera	Vendor Advisory secunia.com Depreciated Link text/plain	SECUNIA 47018
No Description Provided	osvdb.org Inactive Link Not Archived	OSVDB 77387
Bugtraq: Vulnerabilities in 3S CoDeSys 3.4 SP4 Patch 2	seclists.org text/html	BUGTRAQ 20111129 Vulnerabilities in 3S CoDeSys 3.4 SP4 Patch 2

By selecting these links, you may be leaving CVEreport webspace. We have provided these links to other websites because they may have information that would be of interest to you. No inferences should be drawn on account of other sites being referenced, or not, from this page. There may be other websites that are more appropriate for your purpose. CVEreport does not necessarily endorse the views expressed, or concur with the facts presented on these sites. Further, CVEreport does not endorse any commercial products that may be mentioned on these sites. Please address comments about any linked pages to comment@cve.report.

There are currently no QIDs associated with this CVE

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	3ssoftware	Codesys	All	sp4	All	All

cpe:2.3:a:3ssoftware:codesys:*:sp4:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

Social Mentions

Source	Title	Posted (UTC)
/r/snort	Problems disabling low sid Snort rules	2016-10-31 15:18:40

← Previous ID

Next ID→