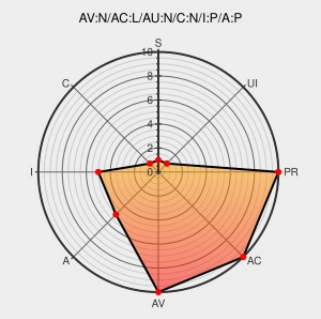
CVE-2011-5058

Published on: 01/10/2012 12:00:00 AM UTC

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

CVE-2011-5058

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



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

The CmbWebserver.dll module of the Control service in 3S CoDeSys 3.4 SP4 Patch 2 allows remote attackers to create arbitrary directories under the web root by specifying a non-existent directory using \ (backslash) characters in an HTTP GET request.

CVE-2011-5058 has been assigned by cve@mitre.org to track the vulnerability

CVSS2 Score: 6.4 - MEDIUM

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

CVE References

Description	Tags	Link
	Exploit, aluigi.altervista.org, text/plain	MISC aluigi.altervista.org/adv/codesys_1-adv.txt
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
About Secunia Research | Flexera	Vendor Advisory, secunia.com, Depreciated Link, text/plain	SECUNIA 47018
IBM X-Force Exchange	exchange.xforce.ibmcloud.com, text/html	XF codesys-cmbwebserver-dir-traversal(72339)

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	3.4	sp4	patch2	All
Application	3ssoftware	Codesys	3.4	sp4	patch2	All

cpe:2.3:a:3ssoftware:codesys:3.4:sp4:patch2:*:*:*:*:*:

cpe:2.3:a:3ssoftware:codesys:3.4:sp4:patch2:*:*:*:*:*:

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→