



CVE-2012-1824

[MITRE](#)[NVD](#)[CVE.ORG](#)[JSON API](#)[Print: PDF](#)

Summary

CVE	CVE-2012-1824
State	PUBLIC
Assigner	cert@cert.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2012-05-25 19:55:00 UTC
Updated	2012-05-28 04:00:00 UTC
Description	Untrusted search path vulnerability in Measuresoft ScadaPro Client before 4.0.0 and ScadaPro Server before 4.0.0 allows I

Risk And Classification

Problem Types: NVD-CWE-Other

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Measuresoft	Scadapro Client	All	All	All	All
Application	Measuresoft	Scadapro Server	All	All	All	All

References

Reference	Source	Link	Tags
404 - File or directory not found.	MISC	www.measuresoft.net	
404 - File or directory not found.	MISC	www.measuresoft.net	
404 - File Not Found CISA	MISC	www.us-cert.gov	US Government Resource
CVE Program record	CVE.ORG	www.cve.org	canonical
NVD vulnerability detail	NVD	nvd.nist.gov	canonical, analysis

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

[590867](#) Measuresoft ScadaPro DLL Hijack Vulnerability (ICSA-12-145-01)

Use of this information constitutes acceptance for use in an AS IS condition. There are NO warranties, implied or otherwise, with regard to this information or its use. Any use of this information is at the user's risk. It is the responsibility of user to evaluate the accuracy, completeness or usefulness of any information, opinion, advice or other content. EACH USER WILL BE SOLELY RESPONSIBLE FOR ANY consequences of his or her direct or indirect use of this web site. ALL WARRANTIES OF ANY KIND ARE EXPRESSLY DISCLAIMED. This site will NOT BE LIABLE FOR ANY DIRECT, INDIRECT or any other kind of loss.

CVE, CWE, and OVAL are registered trademarks of [The MITRE Corporation](#) and the authoritative source of CVE content is [MITRE's CVE web site](#). This site includes MITRE data granted under the following [license](#).

Free CVE JSON API cve.report/api

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