



CVE-2015-0883

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

Summary

CVE	CVE-2015-0883
State	PUBLIC
Assigner	vultures@jpcert.or.jp
Source Priority	CVE Program / NVD first with legacy fallback
Published	2015-02-27 02:59:00 UTC
Updated	2015-02-27 17:34:00 UTC
Description	SYNCK GRAPHICA Mailform Pro CGI 4.1.4 and 4.1.5, when the mailauth module is enabled, does not properly send e-mail

Risk And Classification

Problem Types: NVD-CWE-noinfo

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Synck Graphica	Mailform Pro Cgi	4.1.4	All	All	All
Application	Synck Graphica	Mailform Pro Cgi	4.1.5	All	All	All
Application	Synck Graphica	Mailform Pro Cgi	4.1.4	All	All	All
Application	Synck Graphica	Mailform Pro Cgi	4.1.5	All	All	All

References

Reference	Source	Link	Tags
メールフォームプロ4.2.0公開と脆弱性に関するお知らせ	CONFIRM	www.synck.com	Vendor Advisory
JVNDB-2015-000026	JVNDB	jvndb.jvn.jp	Vendor Advisory
JVN#30135729: SYNCK GRAPHICA Mailform Pro CGI vulnerable to remote code execution	JVN	jvn.jp	Vendor Advisory
Japan Vulnerability Notes/Information from SYNCK GRAPHICA	CONFIRM	jvn.jp	
CVE Program record	CVE.ORG	www.cve.org	canonical
NVD vulnerability detail	NVD	nvd.nist.gov	canonical, authoritative

No vendor comments have been submitted for this CVE.

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

© [CVE.report](#) 2026 |

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](#)