



CVE-2018-0580

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

Summary

CVE	CVE-2018-0580
State	PUBLIC
Assigner	vultures@jpcert.or.jp
Source Priority	CVE Program / NVD first with legacy fallback
Published	2018-05-14 13:29:00 UTC
Updated	2018-06-20 14:50:00 UTC
Description	Untrusted search path vulnerability in CELSYS, Inc CLIP STUDIO series (CLIP STUDIO PAINT (for Windows) EX/PRO/DE

Risk And Classification

Problem Types: CWE-426

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Celsys	Clip Studio Action	All	All	All	All
Application	Celsys	Clip Studio Modeler	All	All	All	All
Application	Celsys	Clip Studio Paint	All	All	All	All

References

Reference	Source	Link
CLIP STUDIO ACTION アップデータのダウンロード CLIP STUDIO	MISC	www.clip-studio.c
Downloads CLIP STUDIO PAINT CLIP STUDIO.NET	MISC	www.clipstudio.ne
JVN#68345747: The installers of multiple CELSYS,Inc. software may insecurely load Dynamic Link Libraries	JVN	jvn.jp
CVE Program record	CVE.ORG	www.cve.org
NVD vulnerability detail	NVD	nvd.nist.gov

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](#)