



CVE-2020-5681

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

Summary

CVE	CVE-2020-5681
State	PUBLIC
Assigner	vultures@jpcert.or.jp
Source Priority	CVE Program / NVD first with legacy fallback
Published	2020-12-24 02:15:00 UTC
Updated	2020-12-30 15:44:00 UTC
Description	Untrusted search path vulnerability in self-extracting files created by EpsonNet SetupManager versions 2.2.14 and earlier, a

Risk And Classification

Problem Types: CWE-427

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Epson	Epsonnet Setupmanager	All	All	All	All
Application	Epson	Epsonnet Setupmanager	All	All	All	All
Application	Epson	Offirio Synergyware Printdirector	All	All	All	All
Application	Epson	Offirio Synergyware Printdirector	All	All	All	All

References

Reference	Source
エプソン製ソフトウェアで作成した自己解凍形式ファイルのDLL読み込みに関する脆弱性について	MISC
JVN#94244575: Self-Extracting files created by multiple SEIKO EPSON products may insecurely load Dynamic Link Libraries	MISC
CVE Program record	CVE.ORG
NVD vulnerability detail	NVD

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](#).

CVE.report and Source URL Uptime Status [status.cve.report](#)