



CVE-2018-0601

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

Summary

CVE	CVE-2018-0601
State	PUBLIC
Assigner	vultures@jpcert.or.jp
Source Priority	CVE Program / NVD first with legacy fallback
Published	2018-06-26 14:29:00 UTC
Updated	2023-11-07 02:51:00 UTC
Description	Untrusted search path vulnerability in axpdfium v0.01 allows an attacker to gain privileges via a Trojan horse DLL in an uns

Risk And Classification

Problem Types: CWE-426

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Axpdfium Project	Axpdfium	0.01	All	All	All
Application	Axpdfium Project	Axpdfium	0.01	All	All	All

References

Reference	Source	Link	Tags
github.com/yak1ex/axpdfium/wiki/JVN%2379301396%28en%29		github.com	
JVN#79301396(en) · yak1ex/axpdfium Wiki · GitHub	MISC	github.com	Patch, Third Party Advisory
JVN#79301396: Susie plug-in "axpdfium" may insecurely load Dynamic Link Libraries	JVN	jvn.jp	Third Party Advisory
Home · yak1ex/axpdfium Wiki · GitHub	MITRE	github.com	
Home · yak1ex/axpdfium Wiki · GitHub	MITRE	github.com	
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.

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](#)