



CVE-2021-40716

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

Summary

CVE	CVE-2021-40716
State	PUBLIC
Assigner	psirt@adobe.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2021-09-29 16:15:00 UTC
Updated	2023-11-07 03:38:00 UTC
Description	XMP Toolkit SDK versions 2021.07 (and earlier) are affected by an out-of-bounds read vulnerability that could lead to disclo

Risk And Classification

Problem Types: CWE-125

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Adobe	Xmp Toolkit Software Development Kit	All	All	All	All
Application	Adobe	Xmp Toolkit Software Development Kit	All	All	All	All
Operating System	Debian	Debian Linux	10.0	All	All	All

References

Reference	Source	Link	Tags
[SECURITY] [DLA 3585-1] exempi security update	MLIST	lists.debian.org	
Adobe Security Bulletin	MISC	helpx.adobe.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.

Legacy QID Mappings

[184372](#) Debian Security Update for exempi (CVE-2021-40716)

[198834](#) Ubuntu Security Notification for Exempi Vulnerabilities (USN-5483-1)

[6000108](#) Debian Security Update for exempi (DLA 3585-1)

© [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](#)