



CVE-2019-14678

[MITRE](#)[NVD](#)[CVE.ORG](#)[JSON API](#)[Print: PDF !\[\]\(003082e50e3009141f59bd5df831749f_img.jpg\)](#)

Summary

CVE	CVE-2019-14678
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2019-11-14 21:15:00 UTC
Updated	2019-11-22 19:34:00 UTC
Description	SAS XML Mapper 9.45 has an XML External Entity (XXE) vulnerability that can be leveraged by malicious attackers in mult

Risk And Classification

Problem Types: CWE-611

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Hp	Hp-ux	-	All	All	All
Operating System	Hp	Hp-ux	-	All	All	All
Operating System	Ibm	Aix	-	All	All	All
Operating System	Ibm	Aix	-	All	All	All
Operating System	Ibm	Z/os	-	All	All	All
Operating System	Ibm	Z/os	-	All	All	All
Operating System	Ibm	Z/os	-	All	All	All
Operating System	Linux	Linux Kernel	-	All	All	All
Operating System	Linux	Linux Kernel	-	All	All	All
Operating System	Microsoft	Windows	-	All	All	All
Operating System	Microsoft	Windows	-	All	All	All
Operating System	Microsoft	Windows 10	-	All	All	All
Operating System	Microsoft	Windows 10	-	All	All	All
Operating System	Microsoft	Windows 7	-	-	All	All
Operating System	Microsoft	Windows 7	-	-	All	All
Operating System	Microsoft	Windows 7	-	-	All	All
Operating System	Microsoft	Windows 7	-	-	All	All

Operating System	Microsoft	Windows 7	-	-	All	All
Operating System	Microsoft	Windows 7	-	-	All	All
Operating System	Microsoft	Windows 7	-	-	All	All
Operating System	Microsoft	Windows 7	-	-	All	All
Operating System	Microsoft	Windows 8	-	All	All	All
Operating System	Microsoft	Windows 8	-	All	All	All
Operating System	Microsoft	Windows 8	-	All	All	All
Operating System	Microsoft	Windows 8	-	All	All	All
Operating System	Microsoft	Windows 8.1	-	All	All	All
Operating System	Microsoft	Windows 8.1	-	All	All	All
Operating System	Microsoft	Windows Server 2012	-	All	All	All
Operating System	Microsoft	Windows Server 2012	-	All	All	All
Operating System	Microsoft	Windows Server 2012	r2	All	All	All
Operating System	Microsoft	Windows Server 2012	-	All	All	All
Operating System	Microsoft	Windows Server 2012	-	All	All	All
Operating System	Microsoft	Windows Server 2012	r2	All	All	All
Operating System	Microsoft	Windows Server 2016	-	All	All	All
Operating System	Microsoft	Windows Server 2016	-	All	All	All
Operating System	Microsoft	Windows Server 2019	-	All	All	All
Operating System	Microsoft	Windows Server 2019	-	All	All	All
Operating System	Oracle	Solaris	-	All	All	All
Operating System	Oracle	Solaris	-	All	All	All
Application	Sas	Base Sas	9.4	ts1m6	All	All
Application	Sas	Base Sas	9.4	ts1m6	All	All
Application	Sas	Xml Mapper	9.45	All	All	All
Application	Sas	Xml Mapper	9.45	All	All	All

References

Reference	Source
64719 - SAS® XML Mapper contains an XML External Entity (XXE) vulnerability that also affects the XMLV2 LIBNAME engine	MISC
Disclosures/CVE-2019-14678-Unsafe XML Parsing-SAS XML Mapper at master · DrunkenShells/Disclosures · GitHub	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](#).

Free CVE JSON API [cve.report/api](#)

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