



CVE-2018-1311

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

Summary

CVE	CVE-2018-1311
State	PUBLIC
Assigner	security@apache.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2019-12-18 20:15:00 UTC
Updated	2023-12-31 14:15:00 UTC
Description	The Apache Xerces-C 3.0.0 to 3.2.3 XML parser contains a use-after-free error triggered during the scanning of external D

Risk And Classification

Problem Types: CWE-416

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Apache	Xerces-c	All	All	All	All
Application	Apache	Xerces-c	All	All	All	All
Application	Apache	Xerces-c	All	All	All	All
Operating System	Debian	Debian Linux	10.0	All	All	All
Operating System	Debian	Debian Linux	9.0	All	All	All
Application	Oracle	Goldengate	All	All	All	All
Operating System	Redhat	Enterprise Linux Desktop	6.0	All	All	All
Operating System	Redhat	Enterprise Linux Desktop	7.0	All	All	All
Operating System	Redhat	Enterprise Linux Eus	7.7	All	All	All
Operating System	Redhat	Enterprise Linux Server	6.0	All	All	All
Operating System	Redhat	Enterprise Linux Server	7.0	All	All	All
Operating System	Redhat	Enterprise Linux Server Aus	7.7	All	All	All
Operating System	Redhat	Enterprise Linux Server Tus	7.7	All	All	All
Operating System	Redhat	Enterprise Linux Workstation	6.0	All	All	All
Operating System	Redhat	Enterprise Linux Workstation	7.0	All	All	All

References

Reference	Source	Link	Tags
Pony Mail!	MLIST	lists.apache.org	Mitigation, Third
Debian -- Security Information -- DSA-4814-1 xerces-c	DEBIAN	www.debian.org	
Pony Mail!		lists.apache.org	
Red Hat Customer Portal	REDHAT	access.redhat.com	
FEDORA-2023-817ecc703f		lists.fedoraproject.org	
Pony Mail!		lists.apache.org	
FEDORA-2023-52ba628e03		lists.fedoraproject.org	
Pony Mail!	MLIST	lists.apache.org	
[SECURITY] [DLA 2498-1] xerces-c security update	MLIST	lists.debian.org	
Oracle Critical Patch Update Advisory - January 2022	MISC	www.oracle.com	
'Xerces-C Security Advisory [CVE-2018-1311]' - MARC	CONFIRM	marc.info	Mailing List, Third
[debian-lts-announce] 20231231 [SECURITY] [DLA 3704-1] xerces-c security update		lists.debian.org	
Pony Mail!		lists.apache.org	
Pony Mail!	MLIST	lists.apache.org	
Red Hat Customer Portal	REDHAT	access.redhat.com	
Pony Mail!		lists.apache.org	
Pony Mail!	MLIST	lists.apache.org	
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

[200042](#) Ubuntu Security Notification for Xerces-C++ Vulnerability (USN-6579-1)

[200052](#) Ubuntu Security Notification for Xerces-C++ Vulnerability (USN-6579-2)

[200056](#) Ubuntu Security Notification for Xerces-C++ Vulnerabilities (USN-6590-1)

[284841](#) Fedora Security Update for xerces (FEDORA-2023-52ba628e03)

[285073](#) Fedora Security Update for xerces (FEDORA-2023-817ecc703f)

[375422](#) IBM Integration Bus and IBM App Connect Enterprise Apache Xerces denial of service Vulnerability(6406232)

[377016](#) Alibaba Cloud Linux Security Update for xerces-c (ALINUX2-SA-2020:0027)

[506277](#) Alpine Linux Security Update for xerces-c

[6000416](#) Debian Security Update for xerces-c (DLA 3704-1)

670213 EulerOS Security Update for xerces-c (EulerOS-SA-2021-1862)
751082 SUSE Enterprise Linux Security Update for xerces-c (SUSE-SU-2021:2920-1)
751088 SUSE Enterprise Linux Security Update for xerces-c (SUSE-SU-2021:2944-1)
751104 OpenSUSE Security Update for xerces-c (openSUSE-SU-2021:1231-1)
751105 OpenSUSE Security Update for xerces-c (openSUSE-SU-2021:2958-1)
755688 SUSE Enterprise Linux Security Update for xerces-c (SUSE-SU-2024:0300-1)
755689 SUSE Enterprise Linux Security Update for xerces-c (SUSE-SU-2024:0299-1)
755696 SUSE Enterprise Linux Security Update for xerces-c (SUSE-SU-2024:0320-1)
900790 Common Base Linux Mariner (CBL-Mariner) Security Update for xerces-c (9201)
901349 Common Base Linux Mariner (CBL-Mariner) Security Update for xerces-c (9201-1)

© [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](#).

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

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