



# CVE-2019-20388

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

## Summary

<b>CVE</b>	CVE-2019-20388
<b>State</b>	PUBLIC
<b>Assigner</b>	cve@mitre.org
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2020-01-21 23:15:00 UTC
<b>Updated</b>	2023-11-09 14:44:00 UTC
<b>Description</b>	xmlSchemaPreRun in xmlschemas.c in libxml2 2.9.10 allows an xmlSchemaValidateStream memory leak.

## Risk And Classification

**Problem Types:** CWE-401

## NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update
Operating System	<a href="#">Debian</a>	<a href="#">Debian Linux</a>	9.0	All
Operating System	<a href="#">Fedoraproject</a>	<a href="#">Fedora</a>	30	All
Operating System	<a href="#">Fedoraproject</a>	<a href="#">Fedora</a>	31	All
Operating System	<a href="#">Fedoraproject</a>	<a href="#">Fedora</a>	32	All
Hardware	<a href="#">Netapp</a>	<a href="#">Baseboard Management Controller H300e</a>	-	All
Operating System	<a href="#">Netapp</a>	<a href="#">Baseboard Management Controller H300e Firmware</a>	-	All
Hardware	<a href="#">Netapp</a>	<a href="#">Baseboard Management Controller H300s</a>	-	All
Operating System	<a href="#">Netapp</a>	<a href="#">Baseboard Management Controller H300s Firmware</a>	-	All
Hardware	<a href="#">Netapp</a>	<a href="#">Baseboard Management Controller H410s</a>	-	All
Operating System	<a href="#">Netapp</a>	<a href="#">Baseboard Management Controller H410s Firmware</a>	-	All
Hardware	<a href="#">Netapp</a>	<a href="#">Baseboard Management Controller H500e</a>	-	All
Operating System	<a href="#">Netapp</a>	<a href="#">Baseboard Management Controller H500e Firmware</a>	-	All
Hardware	<a href="#">Netapp</a>	<a href="#">Baseboard Management Controller H500s</a>	-	All
Operating System	<a href="#">Netapp</a>	<a href="#">Baseboard Management Controller H500s Firmware</a>	-	All
Hardware	<a href="#">Netapp</a>	<a href="#">Baseboard Management Controller H700e</a>	-	All
Operating System	<a href="#">Netapp</a>	<a href="#">Baseboard Management Controller H700e Firmware</a>	-	All
Hardware	<a href="#">Netapp</a>	<a href="#">Baseboard Management Controller H700s</a>	-	All

Operating System	Netapp	Baseboard Management Controller H700s Firmware	-	All
Application	Netapp	Cloud Backup	-	All
Application	Netapp	Clustered Data Ontap	-	All
Hardware	Netapp	H300e	-	All
Operating System	Netapp	H300e Firmware	-	All
Hardware	Netapp	H300s	-	All
Operating System	Netapp	H300s Firmware	-	All
Hardware	Netapp	H410s	-	All
Operating System	Netapp	H410s Firmware	-	All
Hardware	Netapp	H500e	-	All
Operating System	Netapp	H500e Firmware	-	All
Hardware	Netapp	H500s	-	All
Operating System	Netapp	H500s Firmware	-	All
Hardware	Netapp	H700e	-	All
Operating System	Netapp	H700e Firmware	-	All
Hardware	Netapp	H700s	-	All
Operating System	Netapp	H700s Firmware	-	All
Application	Netapp	Ontap Select Deploy Administration Utility	-	All
Application	Netapp	Plug-in For Symantec Netbackup	-	All
Application	Netapp	Smi-s Provider	-	All
Application	Netapp	Snapdrive	-	All
Application	Netapp	Steelstore Cloud Integrated Storage	-	All
Operating System	Opensuse	Leap	15.1	All
Application	Oracle	Communications Cloud Native Core Network Function Cloud Native Environment	1.10.0	All
Application	Oracle	Enterprise Manager Base Platform	13.4.0.0	All
Application	Oracle	Enterprise Manager Base Platform	13.5.0.0	All
Application	Oracle	Enterprise Manager Ops Center	12.4.0.0	All
Application	Oracle	Mysql Workbench	All	All
Application	Oracle	Peoplesoft Enterprise Peopletools	8.58	All
Application	Oracle	Real User Experience Insight	13.3.1.0	All
Application	Oracle	Real User Experience Insight	13.4.1.0	All
Application	Oracle	Real User Experience Insight	13.5.1.0	All
Application	Xmlsoft	Libxml2	2.9.10	All
Application	Xmlsoft	Libxml2	2.9.10	All

## References

Reference	Source	Link
libxml2: Multiple vulnerabilities (GLSA 202010-04) — Gentoo security	GENTOO	<a href="https://security.gentoo.org">security.gentoo.org</a>
[SECURITY] [DLA 2369-1] libxml2 security update	MLIST	<a href="https://lists.debian.org">lists.debian.org</a>
Oracle Critical Patch Update Advisory - July 2020	MISC	<a href="https://www.oracle.com">www.oracle.com</a>
Oracle Critical Patch Update Advisory - April 2022	MISC	<a href="https://www.oracle.com">www.oracle.com</a>
[security-announce] openSUSE-SU-2020:0681-1: moderate: Security update f	SUSE	<a href="https://lists.opensuse.org">lists.opensuse.org</a>
[SECURITY] Fedora 30 Update: libxml2-2.9.10-3.fc30 - package-announce - Fedora Mailing-Lists	FEDORA	<a href="https://lists.fedoraproject.org">lists.fedoraproject.org</a>
Fix memory leak in xmlSchemaValidateStream (I68) · Merge Requests · GNOME / libxml2 · GitLab	MISC	<a href="https://gitlab.gnome.org">gitlab.gnome.org</a>
[SECURITY] Fedora 31 Update: libxml2-2.9.10-3.fc31 - package-announce - Fedora Mailing-Lists	FEDORA	<a href="https://lists.fedoraproject.org">lists.fedoraproject.org</a>
[SECURITY] Fedora 32 Update: mingw-libxml2-2.9.10-1.fc32 - package-announce - Fedora Mailing-Lists		<a href="https://lists.fedoraproject.org">lists.fedoraproject.org</a>
Oracle Critical Patch Update Advisory - October 2021	MISC	<a href="https://www.oracle.com">www.oracle.com</a>
[SECURITY] Fedora 31 Update: libxml2-2.9.10-3.fc31 - package-announce - Fedora Mailing-Lists		<a href="https://lists.fedoraproject.org">lists.fedoraproject.org</a>
June 2020 Libxml2 Vulnerabilities in NetApp Products   NetApp Product Security	CONFIRM	<a href="https://security.netapp.com">security.netapp.com</a>
[SECURITY] Fedora 32 Update: mingw-libxml2-2.9.10-1.fc32 - package-announce - Fedora Mailing-Lists	FEDORA	<a href="https://lists.fedoraproject.org">lists.fedoraproject.org</a>
[SECURITY] Fedora 30 Update: libxml2-2.9.10-3.fc30 - package-announce - Fedora Mailing-Lists		<a href="https://lists.fedoraproject.org">lists.fedoraproject.org</a>
Oracle Critical Patch Update Advisory - July 2022	N/A	<a href="https://www.oracle.com">www.oracle.com</a>
CVE Program record	CVE.ORG	<a href="https://www.cve.org">www.cve.org</a>
NVD vulnerability detail	NVD	<a href="https://nvd.nist.gov">nvd.nist.gov</a>

No vendor comments have been submitted for this CVE.

## Legacy QID Mappings

<a href="#">198409</a> Ubuntu Security Notification for libxml2 vulnerabilities (USN-4991-1)
<a href="#">296065</a> Oracle Solaris 11.4 Support Repository Update (SRU) 39.107.1 Missing (CPUOCT2021)
<a href="#">376204</a> Mysql Workbench Critical Patch Update Oct 2021
<a href="#">377365</a> Alibaba Cloud Linux Security Update for libxml2 (ALINUX3-SA-2022:0018)
<a href="#">377454</a> Alibaba Cloud Linux Security Update for libxml2 (ALINUX2-SA-2020:0149)
<a href="#">500340</a> Alpine Linux Security Update for libxml2
<a href="#">504104</a> Alpine Linux Security Update for libxml2
<a href="#">591406</a> Siemens SIMATIC S7-1500 CPU GNU/Linux subsystem Multiple Vulnerabilities (SSB-439005, ICSA-22-104-13)
<a href="#">690499</a> Free Berkeley Software Distribution (FreeBSD) Security Update for libxml (f5abafc0-fcf6-11ea-8758-e0d55e2a8bf9)
<a href="#">730031</a> IBM MQ Appliance Multiple Vulnerabilities(6403297)

[770068](#) Red Hat OpenShift Container Platform 4.6 Security Update (RHSA-2021:0436)

[900125](#) CBL-Mariner Linux Security Update for libxml2 2.9.10

[903107](#) Common Base Linux Mariner (CBL-Mariner) Security Update for libxml2 (1831)

[940076](#) AlmaLinux Security Update for libxml2 (ALSA-2020:4479)

© [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](#)