



# CVE-2022-22822

[MITRE](#)[NVD](#)[CVE.ORG](#)[Print: PDF !\[\]\(e3f8612927870f2e0f9f5989e6dd3064\_img.jpg\)](#)

## Summary

<b>CVE</b>	CVE-2022-22822
<b>State</b>	PUBLIC
<b>Assigner</b>	cve@mitre.org
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2022-01-10 14:12:00 UTC
<b>Updated</b>	2022-10-06 15:29:00 UTC
<b>Description</b>	addBinding in xmlparse.c in Expat (aka libexpat) before 2.4.3 has an integer overflow.

## Risk And Classification

**Problem Types:** CWE-190

## NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	<a href="#">Debian</a>	<a href="#">Debian Linux</a>	10.0	All	All	All
Operating System	<a href="#">Debian</a>	<a href="#">Debian Linux</a>	11.0	All	All	All
Application	<a href="#">Libexpat Project</a>	<a href="#">Libexpat</a>	All	All	All	All
Application	<a href="#">Siemens</a>	<a href="#">Sinema Remote Connect Server</a>	All	All	All	All
Application	<a href="#">Tenable</a>	<a href="#">Nessus</a>	All	All	All	All

## References

Reference	Source	Link
[R1] Nessus Versions 8.15.3 and 10.1.1 Fix Multiple Third-Party Vulnerabilities - Security Advisory   Tenable®	CONFIRM	<a href="http://www.tenable.com">www.tenable.com</a>
[W.I.P.] lib: Prevent more integer overflows by hartwork · Pull Request #539 · libexpat/libexpat · GitHub	MISC	<a href="https://github.com">github.com</a>
Debian -- Security Information -- DSA-5073-1 expat	DEBIAN	<a href="http://www.debian.org">www.debian.org</a>
oss-security - Expat 2.4.3 released, includes 8 security fixes	MLIST	<a href="http://www.openwall.com">www.openwall.com</a>
Expat: Multiple Vulnerabilities (GLSA 202209-24) — Gentoo security	GENTOO	<a href="https://security.gentoo.org">security.gentoo.org</a>
<a href="https://cert-portal.siemens.com/productcert/pdf/ssa-484086.pdf">cert-portal.siemens.com/productcert/pdf/ssa-484086.pdf</a>	CONFIRM	<a href="https://cert-portal.siemens.com">cert-portal.siemens.com</a>
CVE Program record	CVE.ORG	<a href="http://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

159712 Oracle Enterprise Linux Security Update for expat (ELSA-2022-0951)
159733 Oracle Enterprise Linux Security Update for expat (ELSA-2022-1069)
160232 Oracle Enterprise Linux Security Update for xmlrpc-c (ELSA-2022-7692)
179044 Debian Security Update for expat (DLA 2904-1)
179068 Debian Security Update for expat (DSA 5073-1)
183596 Debian Security Update for expat (CVE-2022-22822)
198671 Ubuntu Security Notification for Expat Vulnerabilities (USN-5288-1)
240155 Red Hat Update for expat (RHSA-2022:0951)
240186 Red Hat Update for expat (RHSA-2022:1069)
240794 Red Hat Update for JBoss Core Services (RHSA-2022:7143)
240835 Red Hat Update for xmlrpc-c (RHSA-2022:7692)
257160 CentOS Security Update for expat (CESA-2022:1069)
296057 Oracle Solaris 11.4 Support Repository Update (SRU) 44.113.4 Missing (bulletinapr2022)
330124 IBM AIX Multiple Vulnerabilities in Python (python_advisory)
353975 Amazon Linux Security Advisory for expat : ALAS-2022-1603
353986 Amazon Linux Security Advisory for expat : ALAS2-2022-1809
354360 Amazon Linux Security Advisory for expat : ALAS2022-2022-017
354434 Amazon Linux Security Advisory for expat : ALAS2022-2022-232
354570 Amazon Linux Security Advisory for expat : ALAS-2022-232
355281 Amazon Linux Security Advisory for expat : ALAS2023-2023-058
376581 F5 BIG-IP Application Security Manager (ASM), Local Traffic Manager (LTM), Access Policy Manager (APM) Expat Vulnerability (K23421535)
376713 Tenable Nessus Multiple Third-Party Vulnerabilities (TNS-2022-05)
377041 Alibaba Cloud Linux Security Update for expat (ALINUX2-SA-2022:0017)
377097 Alibaba Cloud Linux Security Update for expat (ALINUX3-SA-2022:0021)
44025 Juniper Network Operating System (Junos OS) Multiple Vulnerabilities (JSA70605)
500177 Alpine Linux Security Update for expat

501400 Alpine Linux Security Update for expat
501738 Alpine Linux Security Update for expat
503914 Alpine Linux Security Update for expat
591406 Siemens SIMATIC S7-1500 CPU GNU/Linux subsystem Multiple Vulnerabilities (SSB-439005, ICSA-22-104-13)
610429 Google Android Devices September 2022 Security Patch Missing
610431 Google Android September 2022 Security Patch Missing for Samsung
610439 Google Android October 2022 Security Patch Missing for Huawei EMUI
6140071 AWS Bottlerocket Security Update for libexpat (GHSA-4wxx-9rrx-2j9f)
671428 EulerOS Security Update for expat (EulerOS-SA-2022-1342)
671447 EulerOS Security Update for expat (EulerOS-SA-2022-1425)
671459 EulerOS Security Update for expat (EulerOS-SA-2022-1446)
671508 EulerOS Security Update for expat (EulerOS-SA-2022-1502)
671512 EulerOS Security Update for expat (EulerOS-SA-2022-1483)
671657 EulerOS Security Update for xulrunner (EulerOS-SA-2022-1774)
671715 EulerOS Security Update for expat (EulerOS-SA-2022-1716)
710626 Gentoo Linux Expat Multiple Vulnerabilities (GLSA 202209-24)
751651 SUSE Enterprise Linux Security Update for expat (SUSE-SU-2022:0178-1)
751653 SUSE Enterprise Linux Security Update for expat (SUSE-SU-2022:0179-1)
751662 OpenSUSE Security Update for expat (openSUSE-SU-2022:0178-1)
753347 SUSE Enterprise Linux Security Update for expat (SUSE-SU-2022:14878-1)
87486 IBM Hypertext Transfer Protocol Server (HTTP Server) Multiple Vulnerabilities (6559296)
900510 Common Base Linux Mariner (CBL-Mariner) Security Update for expat (7129)
901060 Common Base Linux Mariner (CBL-Mariner) Security Update for expat (7156-1)
904967 Common Base Linux Mariner (CBL-Mariner) Security Update for cmake (12319)
905054 Common Base Linux Mariner (CBL-Mariner) Security Update for cmake (12469)
940473 AlmaLinux Security Update for expat (ALSA-2022:0951)
940736 AlmaLinux Security Update for xmlrpc-c (ALSA-2022:7692)
960622 Rocky Linux Security Update for xmlrpc-c (RLSA-2022:7692)

© [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](#)**