CVE-2022-23852

MITRE | NVD | CVE.ORG | Print: PDF

Summary

CVE	CVE-2022-23852
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2022-01-24 02:15:00 UTC
Updated	2022-10-29 02:44:00 UTC
Description	Expat (aka libexpat) before 2.4.4 has a signed integer overflow in XML_GetBuffer, for configurations with a nonzero XML_C

Risk And Classification

Problem Types: CWE-190

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Debian	Debian Linux	9.0	All	All	All
Application	Libexpat Project	Libexpat	All	All	All	All
Application	Netapp	Clustered Data Ontap	-	All	All	All
Application	Netapp	Oncommand Workflow Automation	-	All	All	All
Application	Oracle	Communications Metasolv Solution	6.3.1	All	All	All
Application	Siemens	Sinema Remote Connect Server	All	All	All	All
Application	Tenable	Nessus	All	All	All	All

References

Reference	Source
[CVE-2022-23852] Prevent XML_GetBuffer signed integer overflow by hartwork · Pull Request #550 · libexpat/libexpat · GitHub	MISC
Oracle Critical Patch Update Advisory - April 2022	MISC
[R1] Nessus Versions 8.15.3 and 10.1.1 Fix Multiple Third-Party Vulnerabilities - Security Advisory | Tenable®	CONFIRM
[SECURITY] [DLA 2935-1] expat security update	MLIST
CVE-2022-23852 Expat Vulnerability in NetApp Products | NetApp Product Security	CONFIRM
Debian -- Security Information -- DSA-5073-1 expat	DEBIAN
Expat: Multiple Vulnerabilities (GLSA 202209-24) — Gentoo security	GENTOO

cert-portal.siemens.com/productcert/pdf/ssa-484086.pdf	CONFIRM
CVE Program record	CVE.ORG
NVD vulnerability detail	NVD

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)
- 179044 Debian Security Update for expat (DLA 2904-1)
- 179068 Debian Security Update for expat (DSA 5073-1)
- 179107 Debian Security Update for expat (DLA 2935-1)
- 182780 Debian Security Update for expat (CVE-2022-23852)
- 198671 Ubuntu Security Notification for Expat Vulnerabilities (USN-5288-1)
- 20253 Oracle Database 12.1.0.2 Critical Patch Update - April 2022
- 20254 Oracle Database 12.1.0.2 Critical Patch Update - April 2022 (Unauthenticated)
- 20255 Oracle Database 19c Critical Patch Update - April 2022
- 20257 Oracle Database 21c Critical Patch Update - April 2022
- 20258 IBM DB2 Arbitrary Code Execution Vulnerability (6573293)
- 20285 Oracle Database 19c Critical OJVM Patch Update - April 2022
- 240155 Red Hat Update for expat (RHSA-2022:0951)
- 240186 Red Hat Update for expat (RHSA-2022:1069)
- 240389 Red Hat Update for expat (RHSA-2022:4834)
- 240794 Red Hat Update for JBoss Core Services (RHSA-2022:7143)
- 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)
- 353176 Amazon Linux Security Advisory for expat : ALAS-2022-1569
- 353182 Amazon Linux Security Advisory for expat : ALAS2-2022-1754
- 354427 Amazon Linux Security Advisory for expat : ALAS2022-2022-028

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

376583 F5 BIG-IP Application Security Manager (ASM), Local Traffic Manager (LTM), Access Policy Manager (APM) Expat Vulnerability (K19473898)

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)

500178 Alpine Linux Security Update for expat

501401 Alpine Linux Security Update for expat

501739 Alpine Linux Security Update for expat

502179 Alpine Linux Security Update for qt5-qtwebengine

502358 Alpine Linux Security Update for qt5-qtwebengine

503915 Alpine Linux Security Update for expat

505363 Alpine Linux Security Update for qt5-qtwebengine

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

6140379 AWS Bottlerocket Security Update for libexpat (GHSA-q23q-h3vx-q22h)

671447 EulerOS Security Update for expat (EulerOS-SA-2022-1425)

671459 EulerOS Security Update for expat (EulerOS-SA-2022-1446)

671565 EulerOS Security Update for expat (EulerOS-SA-2022-1529)

671588 EulerOS Security Update for expat (EulerOS-SA-2022-1562)

671620 EulerOS Security Update for expat (EulerOS-SA-2022-1659)

671642 EulerOS Security Update for expat (EulerOS-SA-2022-1645)

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)

751724 SUSE Enterprise Linux Security Update for expat (SUSE-SU-2022:0495-1)

751730 SUSE Enterprise Linux Security Update for expat (SUSE-SU-2022:0498-1)

751741 OpenSUSE Security Update for expat (openSUSE-SU-2022:0498-1)

753230 SUSE Enterprise Linux Security Update for expat (SUSE-SU-2022:14884-1)

87486 IBM Hypertext Transfer Protocol Server (HTTP Server) Multiple Vulnerabilities (6559296)

87497 IBM HTTP Server Multiple Expat Vulnerabilities

900613 Common Base Linux Mariner (CBL-Mariner) Security Update for expat (7831)

901792 Common Base Linux Mariner (CBL-Mariner) Security Update for expat (7835-1)

904817 Common Base Linux Mariner (CBL-Mariner) Security Update for cmake (12311)

905153 Common Base Linux Mariner (CBL-Mariner) Security Update for cmake (12472)

940473 AlmaLinux Security Update for expat (ALSA-2022:0951)

960848 Rocky Linux Security Update for expat (RLSA-2022:0951)