CVE-2022-43680

MITRE | NVD | CVE.ORG | Print: PDF

Summary

CVE	CVE-2022-43680
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2022-10-24 14:15:00 UTC
Updated	2024-01-21 02:08:00 UTC
Description	In libexpat through 2.4.9, there is a use-after free caused by overeager destruction of a shared DTD in XML_ExternalEntityI

Risk And Classification

Problem Types: CWE-416

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Debian	Debian Linux	10.0	All	All	All
Operating System	Debian	Debian Linux	11.0	All	All	All
Operating System	Fedoraproject	Fedora	35	All	All	All
Operating System	Fedoraproject	Fedora	36	All	All	All
Operating System	Fedoraproject	Fedora	37	All	All	All
Application	Libexpat Project	Libexpat	All	All	All	All
Application	Netapp	Active Iq Unified Manager	-	All	All	All
Hardware	Netapp	Baseboard Management Controller H300s	-	All	All	All
Operating System	Netapp	Baseboard Management Controller H300s Firmware	-	All	All	All
Hardware	Netapp	Baseboard Management Controller H410c	-	All	All	All
Operating System	Netapp	Baseboard Management Controller H410c Firmware	-	All	All	All
Hardware	Netapp	Baseboard Management Controller H410s	-	All	All	All
Operating System	Netapp	Baseboard Management Controller H410s Firmware	-	All	All	All
Hardware	Netapp	Baseboard Management Controller H500s	-	All	All	All
Operating System	Netapp	Baseboard Management Controller H500s Firmware	-	All	All	All
Hardware	Netapp	Baseboard Management Controller H700s	-	All	All	All
Operating System	Netapp	Baseboard Management Controller H700s Firmware	-	All	All	All

Hardware	Netapp	H300s	-	All	All	All
Operating System	Netapp	H300s Firmware	-	All	All	All
Hardware	Netapp	H410c	-	All	All	All
Operating System	Netapp	H410c Firmware	-	All	All	All
Hardware	Netapp	H410s	-	All	All	All
Operating System	Netapp	H410s Firmware	-	All	All	All
Hardware	Netapp	H500s	-	All	All	All
Operating System	Netapp	H500s Firmware	-	All	All	All
Hardware	Netapp	H700s	-	All	All	All
Operating System	Netapp	H700s Firmware	-	All	All	All
Hardware	Netapp	Hci Compute Node	-	All	All	All
Operating System	Netapp	Hci Compute Node Firmware	-	All	All	All
Application	Netapp	Oncommand Workflow Automation	-	All	All	All
Application	Netapp	Solidfire Hci Management Node	-	All	All	All

References

Reference
[SECURITY] Fedora 36 Update: mingw-pixman-0.42.2-1.fc36 - package-announce - Fedora Mailing-Lists
[SECURITY] Fedora 35 Update: mingw-pixman-0.42.2-1.fc35 - package-announce - Fedora Mailing-Lists
[SECURITY] Fedora 35 Update: mingw-expat-2.5.0-1.fc35 - package-announce - Fedora Mailing-Lists
CVE-2022-43680 libexpat Vulnerability in NetApp Products | NetApp Product Security
[CVE-2022-43680] Fix overeager DTD destruction (fixes #649) by hartwork · Pull Request #650 · libexpat/libexpat · GitHub
Bugfixes by c01db33f · Pull Request #616 · libexpat/libexpat · GitHub
[SECURITY] Fedora 36 Update: mingw-pixman-0.42.2-1.fc36 - package-announce - Fedora Mailing-Lists
[SECURITY] Fedora 37 Update: mingw-expat-2.5.0-1.fc37 - package-announce - Fedora Mailing-Lists
[SECURITY] Fedora 37 Update: mingw-pixman-0.42.2-1.fc37 - package-announce - Fedora Mailing-Lists
[SECURITY] Fedora 37 Update: mingw-expat-2.5.0-1.fc37 - package-announce - Fedora Mailing-Lists
[oss-security] 20240103 CVE-2022-43680: Apache OpenOffice: "Use after free" fixed in libexpat
[SECURITY] Fedora 37 Update: mingw-pixman-0.42.2-1.fc37 - package-announce - Fedora Mailing-Lists
[CVE-2022-43680] XML_ParserFree may free parser->m_dtd memory in out-of-memory situations when it should not · Issue #649 · libexpat/lib
[SECURITY] Fedora 35 Update: mingw-expat-2.5.0-1.fc35 - package-announce - Fedora Mailing-Lists
Debian -- Security Information -- DSA-5266-1 expat
[SECURITY] [DLA 3165-1] expat security update
[SECURITY] Fedora 36 Update: mingw-expat-2.5.0-1.fc36 - package-announce - Fedora Mailing-Lists
[SECURITY] Fedora 36 Update: mingw-expat-2.5.0-1.fc36 - package-announce - Fedora Mailing-Lists

[SECURITY] Fedora 35 Update: mingw-pixman-0.42.2-1.fc35 - package-announce - Fedora Mailing-Lists

[oss-security] 20231228 CVE-2022-43680: Apache OpenOffice: "Use after free" fixed in libexpat

Expat: Denial of Service (GLSA 202210-38) — Gentoo security

CVE Program record

NVD vulnerability detail

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

160391 Oracle Enterprise Linux Security Update for expat (ELSA-2023-0103)

160416 Oracle Enterprise Linux Security Update for expat (ELSA-2023-0337)

181170 Debian Security Update for expat (DLA 3165-1)

181180 Debian Security Update for expat (DSA 5266-1)

184467 Debian Security Update for expat (CVE-2022-43680)

199034 Ubuntu Security Notification for Expat Vulnerabilities (USN-5638-2)

199042 Ubuntu Security Notification for Expat Vulnerability (USN-5638-3)

199586 Ubuntu Security Notification for Expat Vulnerabilities (USN-5638-4)

20320 IBM DB2 Multiple Vulnerabilities (6847293)

20354 Oracle Database 19c Critical Patch Update - July 2023

20355 Oracle Database 21c Critical Patch Update - July 2023

20356 Oracle Database 19c Critical OJVM Patch Update - July 2023

241059 Red Hat Update for expat (RHSA-2023:0103)

241098 Red Hat Update for expat (RHSA-2023:0337)

242758 Red Hat Update for expat (RHSA-2024:0421)

283309 Fedora Security Update for mingw (FEDORA-2022-49db80f821)

283310 Fedora Security Update for mingw (FEDORA-2022-c43235716e)

283311 Fedora Security Update for mingw (FEDORA-2022-3cf0e7ebc7)

283312 Fedora Security Update for mingw (FEDORA-2022-ae2559a8f4)

283436 Fedora Security Update for mingw (FEDORA-2022-5f1e2e9016)

283437 Fedora Security Update for mingw (FEDORA-2022-f3a939e960)

330126 IBM AIX Denial of Service (DoS) due to Python (python_advisory3)

350126 IBM AIX Denial of Service (DoS) due to Python (python_advisory3)

354129 Amazon Linux Security Advisory for expat : ALAS2-2022-1885

354260 Amazon Linux Security Advisory for expat : ALAS-2022-1655

354507 Amazon Linux Security Advisory for expat : ALAS2022-2022-261

354533 Amazon Linux Security Advisory for expat : ALAS-2022-261

355053 Amazon Linux Security Advisory for expat : AL2012-2022-377

355281 Amazon Linux Security Advisory for expat : ALAS2023-2023-058

377955 Alibaba Cloud Linux Security Update for expat (ALINUX3-SA-2023:0012)

378374 IBM Hypertext Transfer Protocol (HTTP) Server Denial of Service (DoS) Vulnerabilty (6839161)

378599 Splunk Enterprise Third Party Package Updates for June (SVD-2023-0613)

378677 Oracle Hypertext Transfer Protocol Server (HTTP Server) Server Multiple Vulnerabilities (CPUJUL2023)

502571 Alpine Linux Security Update for expat

502572 Alpine Linux Security Update for expat

503918 Alpine Linux Security Update for expat

610466 Google Android Devices February 2023 Security Patch Missing

610467 Google Android February 2023 Security Patch Missing for Samsung

610473 Google Android March 2023 Security Patch Missing for Huawei EMUI

6140074 AWS Bottlerocket Security Update for libexpat (GHSA-fwxw-x96j-mxgm)

672475 EulerOS Security Update for expat (EulerOS-SA-2023-1008)

672520 EulerOS Security Update for expat (EulerOS-SA-2023-1033)

672566 EulerOS Security Update for expat (EulerOS-SA-2023-1122)

672569 EulerOS Security Update for expat (EulerOS-SA-2023-1098)

672596 EulerOS Security Update for expat (EulerOS-SA-2023-1311)

672660 EulerOS Security Update for expat (EulerOS-SA-2023-1355)

672663 EulerOS Security Update for expat (EulerOS-SA-2023-1383)

710677 Gentoo Linux Expat Denial of Service Vulnerability (GLSA 202210-38)

752762 SUSE Enterprise Linux Security Update for expat (SUSE-SU-2022:3874-1)

752766 SUSE Enterprise Linux Security Update for expat (SUSE-SU-2022:3884-1)

752775 SUSE Enterprise Linux Security Update for expat (SUSE-SU-2022:3912-1)

904340 Common Base Linux Mariner (CBL-Mariner) Security Update for expat (11329)

904347 Common Base Linux Mariner (CBL-Mariner) Security Update for expat (11316)

904370 Common Base Linux Mariner (CBL-Mariner) Security Update for expat (11329-1)

904419 Common Base Linux Mariner (CBL-Mariner) Security Update for expat (11316-1)

940880 AlmaLinux Security Update for expat (ALSA-2023:0103)

940896 AlmaLinux Security Update for expat (ALSA-2023:0337)

960520 Rocky Linux Security Update for expat (RLSA-2023:0337)

960621 Rocky Linux Security Update for expat (RLSA-2023:0103)