CVE-2022-25313

MITRE | NVD | CVE.ORG | Print: PDF

Summary

CVE	CVE-2022-25313
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2022-02-18 05:15:00 UTC
Updated	2023-11-07 03:44:00 UTC
Description	In Expat (aka libexpat) before 2.4.5, an attacker can trigger stack exhaustion in build_model via a large nesting depth in the

Risk And Classification

Problem Types: CWE-674

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	34	All	All	All
Operating System	Fedoraproject	Fedora	35	All	All	All
Application	Libexpat Project	Libexpat	All	All	All	All
Application	Oracle	Http Server	12.2.1.3.0	All	All	All
Application	Oracle	Http Server	12.2.1.4.0	All	All	All
Application	Oracle	Zfs Storage Appliance Kit	8.8	All	All	All
Application	Siemens	Sinema Remote Connect Server	All	All	All	All

References

Reference	Source	Link
[CVE-2022-25313] lib: Prevent stack exhaustion in build_model by ferivoz · Pull Request #558 · libexpat/libexpat · GitHub	MISC	githu
Oracle Critical Patch Update Advisory - April 2022	MISC	www
February 2022 Expat Vulnerabilities in NetApp Products | NetApp Product Security	CONFIRM	secu
[SECURITY] Fedora 35 Update: mingw-expat-2.4.6-1.fc35 - package-announce - Fedora Mailing-Lists	FEDORA	lists.
[SECURITY] [DLA 2935-1] expat security update	MLIST	lists.

[SECURITY] Fedora 35 Update: mingw-expat-2.4.6-1.fc35 - package-announce - Fedora Mailing-Lists		lists.
oss-security - Expat 2.4.5 released, includes 5 security fixes	MLIST	www
[SECURITY] Fedora 34 Update: mingw-expat-2.4.6-1.fc34 - package-announce - Fedora Mailing-Lists		lists.
Expat: Multiple Vulnerabilities (GLSA 202209-24) — Gentoo security	GENTOO	secu
Debian -- Security Information -- DSA-5085-1 expat	DEBIAN	www
cert-portal.siemens.com/productcert/pdf/ssa-484086.pdf	CONFIRM	cert-
[SECURITY] Fedora 34 Update: mingw-expat-2.4.6-1.fc34 - package-announce - Fedora Mailing-Lists	FEDORA	lists.
CVE Program record	CVE.ORG	www
NVD vulnerability detail	NVD	nvd.r

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

- 159918 Oracle Enterprise Linux Security Update for expat (ELSA-2022-5314)
- 159925 Oracle Enterprise Linux Security Update for expat (ELSA-2022-5244)
- 179091 Debian Security Update for expat (DSA 5085-1)
- 179107 Debian Security Update for expat (DLA 2935-1)
- 184643 Debian Security Update for expat (CVE-2022-25313)
- 20259 IBM DB2 Multiple Vulnerabilities (6597637)
- 240497 Red Hat Update for expat (RHSA-2022:5244)
- 240505 Red Hat Update for expat (RHSA-2022:5314)
- 240794 Red Hat Update for JBoss Core Services (RHSA-2022:7143)
- 282449 Fedora Security Update for mingw (FEDORA-2022-3d9d67f558)
- 282450 Fedora Security Update for mingw (FEDORA-2022-04f206996b)
- 296057 Oracle Solaris 11.4 Support Repository Update (SRU) 44.113.4 Missing (bulletinapr2022)
- 330124 IBM AIX Multiple Vulnerabilities in Python (python_advisory)
- 354434 Amazon Linux Security Advisory for expat : ALAS2022-2022-232
- 354490 Amazon Linux Security Advisory for expat : ALAS2022-2022-036
- 354570 Amazon Linux Security Advisory for expat : ALAS-2022-232
- 355281 Amazon Linux Security Advisory for expat : ALAS2023-2023-058
- 356393 Amazon Linux Security Advisory for expat : ALAS2-2023-2280

377580 Alibaba Cloud Linux Security Update for expat (ALINUX3-SA-2022:0128)

377786 Alibaba Cloud Linux Security Update for mingw-expat (ALINUX3-SA-2022:0183)

38862 NetApp Data Open Network Technology for Appliance Products (ONTAP) Denial of Service (DoS) Vulnerability (NTAP-20210303-0002)

44025 Juniper Network Operating System (Junos OS) Multiple Vulnerabilities (JSA70605)

500179 Alpine Linux Security Update for expat

501402 Alpine Linux Security Update for expat

501740 Alpine Linux Security Update for expat

503916 Alpine Linux Security Update for expat

591406 Siemens SIMATIC S7-1500 CPU GNU/Linux subsystem Multiple Vulnerabilities (SSB-439005, ICSA-22-104-13)

6140364 AWS Bottlerocket Security Update for libexpat (GHSA-x6p7-99mx-mwxq)

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

671757 EulerOS Security Update for expat (EulerOS-SA-2022-1786)

671760 EulerOS Security Update for expat (EulerOS-SA-2022-1803)

671787 EulerOS Security Update for expat (EulerOS-SA-2022-1861)

671796 EulerOS Security Update for expat (EulerOS-SA-2022-1837)

673085 EulerOS Security Update for expat (EulerOS-SA-2023-2143)

710626 Gentoo Linux Expat Multiple Vulnerabilities (GLSA 202209-24)

751782 SUSE Enterprise Linux Security Update for expat (SUSE-SU-2022:0698-1)

751795 SUSE Enterprise Linux Security Update for expat (SUSE-SU-2022:0713-1)

751810 OpenSUSE Security Update for expat (openSUSE-SU-2022:0713-1)

752302 SUSE Enterprise Linux Security Update for expat (SUSE-SU-2022:2294-1)

753324 SUSE Enterprise Linux Security Update for expat (SUSE-SU-2022:14903-1)

87487 IBM Hypertext Transfer Protocol Server (HTTP Server) Multiple Vulnerabilities (6560814)

900697 Common Base Linux Mariner (CBL-Mariner) Security Update for expat (8629)

901725 Common Base Linux Mariner (CBL-Mariner) Security Update for expat (8623-1)

940591 AlmaLinux Security Update for expat (ALSA-2022:5314)

940631 AlmaLinux Security Update for expat (ALSA-2022:5244)

940738 AlmaLinux Security Update for mingw-expat (ALSA-2022:7811)

960442 Rocky Linux Security Update for expat (RLSA-2022:5314)