CVE-2021-45960

MITRE | NVD | CVE.ORG | Print: PDF

Summary

CVE	CVE-2021-45960
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2022-01-01 19:15:00 UTC
Updated	2022-10-06 19:08:00 UTC
Description	In Expat (aka libexpat) before 2.4.3, a left shift by 29 (or more) places in the storeAtts function in xmlparse.c can lead to rea

Risk And Classification

Problem Types: CWE-682

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
Application	Libexpat Project	Libexpat	All	All	All	All
Application	Netapp	Active Iq Unified Manager	-	All	All	All
Application	Netapp	Hci Baseboard Management Controller	h610c	All	All	All
Application	Netapp	Hci Baseboard Management Controller	h610s	All	All	All
Application	Netapp	Hci Baseboard Management Controller	h615c	All	All	All
Application	Netapp	Hci Management Node	-	All	All	All
Application	Netapp	Oncommand Workflow Automation	-	All	All	All
Application	Netapp	Solidfire	-	All	All	All
Application	Netapp	Solidfire Hci Management Node	-	All	All	All
Application	Siemens	Sinema Remote Connect Server	All	All	All	All
Application	Tenable	Nessus	All	All	All	All

References

Reference
[W.I.P.] lib: Detect and prevent troublesome left shifts in function storeAtts (fixes #531) by hartwork · Pull Request #534 · libexpat/libexpat · Git

[R1] Nessus Versions 8.15.3 and 10.1.1 Fix Multiple Third-Party Vulnerabilities - Security Advisory | Tenable®

CVE-2021-45960 Expat Vulnerability in NetApp Products | NetApp Product Security

Access Denied

A large number of prefixed XML attributes on a single tag can crash libexpat (troublesome left shifts by >=29 bits in function storeAtts) · Issue

Debian -- Security Information -- DSA-5073-1 expat

oss-security - Expat 2.4.3 released, includes 8 security fixes

Expat: Multiple Vulnerabilities (GLSA 202209-24) — Gentoo security

cert-portal.siemens.com/productcert/pdf/ssa-484086.pdf

CVE Program record

NVD vulnerability detail

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)

182190 Debian Security Update for expat (CVE-2021-45960)

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)

257160 CentOS Security Update for expat (CESA-2022:1069)

330124 IBM AIX Multiple Vulnerabilities in Python (python_advisory)

353268 Amazon Linux Security Advisory for expat : ALAS2-2022-1788

353951 Amazon Linux Security Advisory for expat : ALAS-2022-1588

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

376579 F5 BIG-IP Application Security Manager (ASM), Local Traffic Manager (LTM), Access Policy Manager (APM) Expat Vulnerability (K91589041)

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)

6140149 AWS Bottlerocket Security Update for libexpat (GHSA-gmwc-j47g-qq78)

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)

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

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)

900507 Common Base Linux Mariner (CBL-Mariner) Security Update for expat (7114)

901221 Common Base Linux Mariner (CBL-Mariner) Security Update for expat (7124-1)

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

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