CVE-2024-45492

MITRE | NVD | CVE.ORG | JSON API | Print: PDF

Summary

CVE	CVE-2024-45492
State	PUBLISHED
Assigner	mitre
Source Priority	CVE Program / NVD first with legacy fallback
Published	2024-08-30 03:15:03 UTC
Updated	2026-05-12 12:17:10 UTC
Description	An issue was discovered in libexpat before 2.6.3. nextScaffoldPart in xmlparse.c can have an integer overflow for m_groups

Risk And Classification

Primary CVSS: v3.1 9.8 CRITICAL from nvd@nist.gov

CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H

EPSS: 0.022690000 probability, percentile 0.847690000 (date 2026-05-12)

Problem Types: CWE-190 | n/a | CWE-190 CWE-190 Integer Overflow or Wraparound

Version	Source	Type	Score	Severity	Vector
3.1	nvd@nist.gov	Primary	9.8	CRITICAL	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H
3.1	ADP	DECLARED	7.3	HIGH	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:L/A:L
3.1	134c704f-9b21-4f2e-91b3-4a467353bcc0	Secondary	7.3	HIGH	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:L/A:L

CVSS v3.1 Breakdown

Attack Vector

Network

Attack Complexity

Low

Privileges Required

None

User Interaction

None

Scope

Unchanged

Confidentiality

High

ntegrity

High

Availability

High

CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Libexpat Project	Libexpat	All	All	All	All

Vendor Declared Affected Products

Source	Vendor	Product	Version	Platforms
CNA	Na	N/a	affected n/a	Not specified
ADP	Libexpat	Expat	affected 2.6.3 custom	Not specified
ADP	Siemens	RUGGEDCOM RST2428P	affected V3.1 custom	Not specified
ADP	Siemens	SCALANCE XC-300/XR-300/XC-400/XR-500WG/XR-500 Family	unaffected * custom	Not specified
ADP	Siemens	SCALANCE XCM-/XRM-/XCH-/XRH-300 Family	affected V3.1 custom	Not specified
ADP	Siemens	SIMATIC S7-1500 CPU 1518-4 PN/DP MFP	affected V3.1.5 * custom	Not specified
ADP	Siemens	SIMATIC S7-1500 CPU 1518-4 PN/DP MFP	affected V3.1.5 * custom	Not specified
ADP	Siemens	SIMATIC S7-1500 CPU 1518F-4 PN/DP MFP	affected V3.1.5 * custom	Not specified
ADP	Siemens	SIMATIC S7-1500 CPU 1518F-4 PN/DP MFP	affected V3.1.5 * custom	Not specified
ADP	Siemens	SIPLUS S7-1500 CPU 1518-4 PN/DP MFP	affected V3.1.5 * custom	Not specified

References

Reference	Source	Link	Tags
cert-portal.siemens.com/productcert/html/ssa-082556.html	0b142b55-0307-4c5a-b3c9-f314f3fb7c5e	cert-portal.siemens.com	
lists.debian.org/debian-lts-announce/2024/09/msg00036.html	af854a3a-2127-422b-91ae-364da2661108	lists.debian.org	
security.netapp.com/advisory/ntap-20241018-0005	af854a3a-2127-422b-91ae-364da2661108	security.netapp.com	
github.com/libexpat/libexpat/pull/892	cve@mitre.org	github.com	Patch
cert-portal.siemens.com/productcert/html/ssa-613116.html	0b142b55-0307-4c5a-b3c9-f314f3fb7c5e	cert-portal.siemens.com	
github.com/libexpat/libexpat/issues/889	cve@mitre.org	github.com	Issue
CVE Program record	CVE.ORG	www.cve.org	canon
NVD vulnerability detail	NVD	nvd.nist.gov	canon

No vendor comments have been submitted for this CVE.

There are currently no legacy QID mappings associated with this CVE.

© 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 registred 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.

Free CVE JSON API cve.report/api

CVE.report and Source URL Uptime Status **status.cve.report**