CVE-2017-5969

MITRE | NVD | CVE.ORG | Print: PDF

Summary

CVE	CVE-2017-5969
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2017-04-11 16:59:00 UTC
Updated	2023-11-07 02:49:00 UTC
Description	** DISPUTED ** libxml2 2.9.4, when used in recover mode, allows remote attackers to cause a denial of service (NULL poi

Risk And Classification

Problem Types: CWE-476

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Xmlsoft	Libxml2	2.9.4	All	All	All
Application	Xmlsoft	Libxml2	2.9.4	All	All	All

References

Reference	Source	Link
oss-security - CVE request: Null pointer derefence parsing xml file using libxml 2.9.4 (in recover mode)	MLIST	www.openwall.com
[SECURITY] [DLA 2972-1] libxml2 security update	MLIST	lists.debian.org
libxml2: Multiple vulnerabilities (GLSA 201711-01) — Gentoo security	GENTOO	security.gentoo.org
oss-security - CVE-2017-5969: Null pointer derefence parsing xml file using libxml 2.9.4 (in recover mode)	MLIST	www.openwall.com
libxml2 CVE-2017-5969 Null Pointer Dereference Denial of Service Vulnerability	BID	www.securityfocus.c
Bug 778519 – CVE-2017-5969: null pointer dereference when parsing a xml file using recover mode	MISC	bugzilla.gnome.org
CVE Program record	CVE.ORG	www.cve.org
NVD vulnerability detail	NVD	nvd.nist.gov

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

179176 Debian Security Update for libxml2 (DLA 2972-1)

500348 Alpine Linux Security Update for libxml2

504111 Alpine Linux Security Update for libxml2

710359 Gentoo Linux libxml2 Multiple Vulnerabilities (GLSA 201711-01)