CVE-2021-42260

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

Summary

CVE	CVE-2021-42260
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2021-10-11 20:15:00 UTC
Updated	2024-01-12 03:15:00 UTC
Description	TinyXML through 2.6.2 has an infinite loop in TiXmlParsingData::Stamp in tinyxmlparser.cpp via the TIXML_UTF_LEAD_0

Risk And Classification

Problem Types: CWE-835

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	9.0	All	All	All
Application	Tinyxml Project	Tinyxml	2.3.0	beta	All	All
Application	Tinyxml Project	Tinyxml	2.3.1	beta	All	All
Application	Tinyxml Project	Tinyxml	All	All	All	All

References

Reference	Source	Link	Tag
[SECURITY] [DLA 3130-1] tinyxml security update	MLIST	lists.debian.org	
FEDORA-2024-80e6578a01		lists.fedoraproject.org	
TinyXML / Bugs / #141 TIXML_UTF_LEAD_0 can cause TinyXML DoS	MISC	sourceforge.net	
[SECURITY] Fedora 38 Update: tinyxml-2.6.2-28.fc38 - package-announce - Fedora Mailing-Lists		lists.fedoraproject.org	
[SECURITY] [DLA 2988-1] tinyxml security update	MLIST	lists.debian.org	
CVE Program record	CVE.ORG	www.cve.org	canc
NVD vulnerability detail	NVD	nvd.nist.gov	canc

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

- 179254 Debian Security Update for tinyxml (DLA 2988-1)
- 181089 Debian Security Update for tinyxml (DLA 3130-1)
- 181348 Debian Security Update for tinyxml (CVE-2021-42260)
- 199989 Ubuntu Security Notification for TinyXML Vulnerability (USN-6542-1)
- 284854 Fedora Security Update for tinyxml (FEDORA-2024-c9dc0ac419)
- 285065 Fedora Security Update for tinyxml (FEDORA-2024-80e6578a01)
- 751341 OpenSUSE Security Update for tinyxml (openSUSE-SU-2021:3639-1)
- 751351 OpenSUSE Security Update for tinyxml (openSUSE-SU-2021:1474-1)