CVE-2017-7375

MITRE | NVD | CVE.ORG | Print: PDF

Summary

CVE	CVE-2017-7375
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2018-02-19 19:29:00 UTC
Updated	2018-03-18 14:17:00 UTC
Description	A flaw in libxml2 allows remote XML entity inclusion with default parser flags (i.e., when the caller did not request entity sub

Risk And Classification

Problem Types: CWE-611

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Debian	Debian Linux	7.0	All	All	All
Operating System	Debian	Debian Linux	8.0	All	All	All
Operating System	Debian	Debian Linux	9.0	All	All	All
Operating System	Debian	Debian Linux	7.0	All	All	All
Operating System	Debian	Debian Linux	8.0	All	All	All
Operating System	Debian	Debian Linux	9.0	All	All	All
Operating System	Google	Android	4.4.4	All	All	All
Operating System	Google	Android	5.0.2	All	All	All
Operating System	Google	Android	5.1.1	All	All	All
Operating System	Google	Android	6.0	All	All	All
Operating System	Google	Android	6.0.1	All	All	All
Operating System	Google	Android	7.0	All	All	All
Operating System	Google	Android	7.1.1	All	All	All
Operating System	Google	Android	7.1.2	All	All	All
Operating System	Google	Android	4.4.4	All	All	All
Operating System	Google	Android	5.0.2	All	All	All
Operating System	Google	Android	5.1.1	All	All	All

Operating System	Google	Android	6.0	All	All	All
Operating System	Google	Android	6.0.1	All	All	All
Operating System	Google	Android	7.0	All	All	All
Operating System	Google	Android	7.1.1	All	All	All
Operating System	Google	Android	7.1.2	All	All	All
Application	Xmlsoft	Libxml2	2.9.4	rc1	All	All
Application	Xmlsoft	Libxml2	2.9.4	rc2	All	All
Application	Xmlsoft	Libxml2	2.9.4	rc1	All	All
Application	Xmlsoft	Libxml2	2.9.4	rc2	All	All
Application	Xmlsoft	Libxml2	All	All	All	All

References

Reference
libxml2: Multiple vulnerabilities (GLSA 201711-01) — Gentoo security
Android Security Bulletin—June 2017 | Android Open Source Project
1462203 – (CVE-2017-7375) CVE-2017-7375 libxml2: Missing validation for external entities in xmlParsePEReference
Google Android Libraries Multiple Remote Code Execution Vulnerabilities
Prevent unwanted external entity reference (90ccb582) · Commits · GNOME / libxml2 · GitLab
Google Android Multiple Flaws Let Remote Users Deny Service, Obtain Potentially Sensitive Information, and Execute Arbitrary Code and Let
308396a55280f69ad4112d4f9892f4cbeff042aa - platform/external/libxml2 - Git at Google
Debian -- Security Information -- DSA-3952-1 libxml2
CVE Program record
NVD vulnerability detail

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

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

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

904874 Common Base Linux Mariner (CBL-Mariner) Security Update for gettext (12336)

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