CVE-2016-1762

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

Summary

CVE	CVE-2016-1762
State	PUBLISHED
Assigner	apple
Source Priority	CVE Program / NVD first with legacy fallback
Published	2016-03-24 01:59:30 UTC
Updated	2026-05-06 22:30:45 UTC
Description	The xmlNextChar function in libxml2 before 2.9.4 allows remote attackers to cause a denial of service (heap-based buffer o

Risk And Classification

Primary CVSS: v3.1 8.1 HIGH from ADP

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

Problem Types: CWE-119 | CWE-122 | n/a | CWE-122 CWE-122 Heap-based Buffer Overflow

Version	Source	Type	Score	Severity	Vector
3.1	ADP	DECLARED	8.1	HIGH	CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:N/A:H
3.1	134c704f-9b21-4f2e-91b3-4a467353bcc0	Secondary	8.1	HIGH	CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:N/A:H
3.0	nvd@nist.gov	Primary	8.1	HIGH	CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:N/A:H
2.0	nvd@nist.gov	Primary	5.8		AV:N/AC:M/Au:N/C:P/I:N/A:P

CVSS v3.1 Breakdown

Attack Vector

Network

Attack Complexity

Low

Privileges Required

None

User Interaction

Required

Scope

Unchanged

Confidentiality

High

High

Integrity

None

Availability

High

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

CVSS v3.0 Breakdown

Attack Vector

Network

Attack Complexity

Low

Privileges Required

None

User Interaction

Required

Scope

Unchanged

Confidentiality

High

Integrity

None

Availability

High

CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:N/A:H

CVSS v2.0 Breakdown

Access Vector

Network

Access Complexity

Medium

Authentication

None

Confidentiality

Partial

Integrity

None

Availability

Partial

AV:N/AC:M/Au:N/C:P/I:N/A:P

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Apple	Iphone Os	All	All	All	All
Operating System	Apple	Mac Os X	All	All	All	All
Application	Apple	Safari	All	All	All	All
Operating System	Apple	Tvos	All	All	All	All
Operating System	Apple	Watchos	All	All	All	All
Operating System	Canonical	Ubuntu Linux	12.04	All	All	All
Operating System	Canonical	Ubuntu Linux	14.04	All	All	All
Operating System	Canonical	Ubuntu Linux	15.10	All	All	All
Operating System	Canonical	Ubuntu Linux	16.04	All	All	All
Operating System	Debian	Debian Linux	8.0	All	All	All
Application	Mcafee	Web Gateway	All	All	All	All
Application	Mcafee	Web Gateway	All	All	All	All
Operating System	Redhat	Enterprise Linux Desktop	6.0	All	All	All
Operating System	Redhat	Enterprise Linux Desktop	7.0	All	All	All
Operating System	Redhat	Enterprise Linux Server	6.0	All	All	All
Operating System	Redhat	Enterprise Linux Server	7.0	All	All	All
Operating System	Redhat	Enterprise Linux Server Aus	7.2	All	All	All
Operating System	Redhat	Enterprise Linux Server Aus	7.3	All	All	All
Operating System	Redhat	Enterprise Linux Server Aus	7.4	All	All	All
Operating System	Redhat	Enterprise Linux Server Aus	7.6	All	All	All
Operating System	Redhat	Enterprise Linux Server Eus	7.2	All	All	All
Operating System	Redhat	Enterprise Linux Server Eus	7.3	All	All	All
Operating System	Redhat	Enterprise Linux Server Eus	7.4	All	All	All
Operating System	Redhat	Enterprise Linux Server Eus	7.5	All	All	All
Operating System	Redhat	Enterprise Linux Server Eus	7.6	All	All	All
Operating System	Redhat	Enterprise Linux Server Tus	7.2	All	All	All
Operating System	Redhat	Enterprise Linux Server Tus	7.3	All	All	All
Operating System	Redhat	Enterprise Linux Server Tus	7.6	All	All	All
Operating System	Redhat	Enterprise Linux Workstation	6.0	All	All	All
Operating System	Redhat	Enterprise Linux Workstation	7.0	All	All	All
Application	Xmlsoft	Libxml2	All	All	All	All

Vendor Declared Affected Products

Source	Vendor	Product	Version	Platforms

CNA	Na	N/a	affected n/a	Not specified

References

Reference
McAfee Security Bulletin: McAfee Web Gateway update fixes several vulnerabilities related to xml parsing
APPLE-SA-2016-03-21-6 Safari 9.1
Releases
About the security content of tvOS 9.2 - Apple Support
USN-2994-1: libxml2 vulnerabilities | Ubuntu
APPLE-SA-2016-03-21-3 tvOS 9.2
About the security content of Safari 9.1 - Apple Support
Red Hat Customer Portal
Oracle VM Server for x86 Bulletin - July 2016
libxml2 CVE-2016-1762 Multiple Memory Corruption Vulnerabilities
APPLE-SA-2016-03-21-1 iOS 9.3
About the security content of OS X El Capitan v10.11.4 and Security Update 2016-002 - Apple Support
Oracle Linux Bulletin - July 2016
About the security content of watchOS 2.2 - Apple Support
APPLE-SA-2016-03-21-2 watchOS 2.2
Red Hat Customer Portal
Heap-based buffer overread in xmlNextChar (a7a94612) · Commits · GNOME / libxml2 · GitLab
Debian -- Security Information -- DSA-3593-1 libxml2
APPLE-SA-2016-03-21-5 OS X El Capitan 10.11.4 and Security Update 2016-002
Apple iOS Multiple Flaws Let Remote Users Execute Arbitrary Code and Let Remote and Local Users Obtain Potentially Sensitive Information
About the security content of iOS 9.3 - Apple Support
Bug 759671 – Heap-based buffer overread in xmlNextChar (from parser.c:8472)
CVE Program record
NVD vulnerability detail

No vendor comments have been submitted for this CVE.

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

Free CVE JSON API cve.report/api

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