

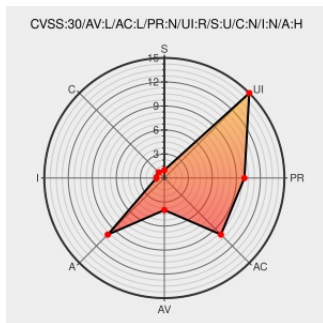


CVE-2016-1839

Published on: 05/20/2016 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:27:04 PM UTC

CVE-2016-1839

[Source: Mitre](#)[Source: NIST](#)[CVE.ORG](#)[Print: PDF](#) 

Certain versions of [Iphone Os](#) from [Apple](#) contain the following vulnerability:

The xmlDictAddString function in libxml2 before 2.9.4, as used in Apple iOS before 9.3.2, OS X before 10.11.5, tvOS before 9.2.1, and watchOS before 2.2.1, allows remote attackers to cause a denial of service (heap-based buffer over-read) via a crafted XML document.

CVE-2016-1839 has been assigned by product-security@apple.com to track the vulnerability - currently rated as **MEDIUM** severity.

CVSS3 Score: **5.5 - MEDIUM**

Attack Vector	Attack Complexity	Privileges Required	User Interaction
LOCAL	LOW	NONE	REQUIRED
Scope	Confidentiality Impact	Integrity Impact	Availability Impact
UNCHANGED	NONE	NONE	HIGH

CVSS2 Score: **4.3 - MEDIUM**

Access Vector	Access Complexity	Authentication
NETWORK	MEDIUM	NONE
Confidentiality Impact	Integrity Impact	Availability Impact
NONE	NONE	PARTIAL

CVE References

Description	Tags	Link
About the security content of OS X El Capitan v10.11.5 and Security Update 2016-003 - Apple Support	Vendor Advisory support.apple.com/text/html	CONFIRM support.apple.com/HT206567
Apple Mac OS X/watchOS/iOS/tvOS	Third Party Advisory	BID 90691

Multiple Security Vulnerabilities	VDB Entry cve.report (archive) text/html	
APPLE-SA-2016-05-16-2 iOS 9.3.2	Mailing List Vendor Advisory lists.apple.com text/html	 APPLE APPLE-SA-2016-05-16-2
USN-2994-1: libxml2 vulnerabilities Ubuntu	Third Party Advisory www.ubuntu.com text/html	 UBUNTU USN-2994-1
APPLE-SA-2016-05-16-4 OS X El Capitan 10.11.5 and Security Update 2016-003	Mailing List Vendor Advisory lists.apple.com text/html	 APPLE APPLE-SA-2016-05-16-4
Debian -- Security Information -- DSA-3593-1 libxml2	Third Party Advisory www.debian.org Deprecated Link text/html	 DEBIAN DSA-3593
Oracle Linux Bulletin - July 2016	Third Party Advisory web.archive.org text/html Inactive Link Not Archived	 CONFIRM www.oracle.com/technetwork/topics/security/linuxbulletinjul2016-3090544.html
Apple iOS Multiple Flaws Let Remote Users Execute Arbitrary Code and Deny Service and Let Remote and Local Users Obtain Potentially Sensitive Information - SecurityTracker	Third Party Advisory VDB Entry www.securitytracker.com text/html	 SECTRAK 1035890
Apple - Lists.apple.com	Mailing List Vendor Advisory lists.apple.com text/html	 APPLE APPLE-SA-2016-05-16-1
Bug 758605 – Heap-based buffer overread in xmlDictAddString	Exploit Issue Tracking Third Party Advisory bugzilla.gnome.org text/html	 CONFIRM bugzilla.gnome.org/show_bug.cgi?id=758605
[R7] LCE 4.8.1 Fixes Multiple Vulnerabilities - Security Advisory Tenable™	Third Party Advisory www.tenable.com text/html	 CONFIRM www.tenable.com/security/tns-2016-18
About the security content of tvOS 9.2.1 - Apple Support	Vendor Advisory support.apple.com text/html	 CONFIRM support.apple.com/HT206564
McAfee Security Bulletin: McAfee Web Gateway update fixes several vulnerabilities related to xml parsing	Patch Third Party Advisory kc.mcafee.com text/html	 CONFIRM kc.mcafee.com/corporate/index?page=content&id=SB10170
Red Hat Customer Portal	Third Party Advisory access.redhat.com text/html	 REDHAT RHSA-2016:1292
Oracle VM Server for x86 Bulletin - July 2016	Third Party Advisory web.archive.org text/html Inactive Link Not Archived	 CONFIRM www.oracle.com/technetwork/topics/security/ovmbulletinjul2016-3090546.html
Bug 758605: Heap-based buffer overread in	Patch	 CONFIRM git.gnome.org/browse/libxml2/commit/?

bug / 00000: heap based buffer overflow in xmlDictAddString... (a820dbea) · Commits · GNOME / libxml2 · GitLab	Patch Third Party Advisory git.gnome.org text/html	 CONFIRM git.gnome.org/browse/libxml2/commit?id=a820dbeac29d330bae4be05d9ecd939ad6b4aa33
Releases	Release Notes Vendor Advisory xmlsoft.org text/xml	 CONFIRM xmlsoft.org/news.html
libxml2: Multiple vulnerabilities (GLSA 201701-37) — Gentoo security	Third Party Advisory security.gentoo.org text/html	 GENTOO GLSA-201701-37
APPLE-SA-2016-05-16-3 watchOS 2.2.1	Mailing List Vendor Advisory lists.apple.com text/html	 APPLE APPLE-SA-2016-05-16-3
About the security content of iOS 9.3.2 - Apple Support	Vendor Advisory support.apple.com text/html	 CONFIRM support.apple.com/HT206568
Google Android Multiple Flaws Let Remote Users Deny Service, Obtain Potentially Sensitive Information, and Execute Arbitrary Code and Let Local Apps Gain Elevated Privileges - SecurityTracker	Third Party Advisory VDB Entry www.securitytracker.com text/html	 SECTRAK 1038623
About the security content of watchOS 2.2.1 - Apple Support	Vendor Advisory support.apple.com text/html	 CONFIRM support.apple.com/HT206566
Red Hat Customer Portal	Third Party Advisory web.archive.org text/html Inactive Link Not Archived	 REDHAT RHSA-2016:2957
Oracle Solaris Bulletin - July 2016	Third Party Advisory www.oracle.com text/html	 CONFIRM www.oracle.com/technetwork/topics/security/bulletinjul2016-3090568.html
By selecting these links, you may be leaving CVEreport webspace. We have provided these links to other websites because they may have information that would be of interest to you. No inferences should be drawn on account of other sites being referenced, or not, from this page. There may be other websites that are more appropriate for your purpose. CVEreport does not necessarily endorse the views expressed, or concur with the facts presented on these sites. Further, CVEreport does not endorse any commercial products that may be mentioned on these sites. Please address comments about any linked pages to comment@cve.report .		

There are currently no QIDs associated with this CVE

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Apple	Iphone Os	All	All	All	All
Operating System	Apple	Iphone Os	All	All	All	All
Operating System	Apple	Mac Os X	All	All	All	All
Operating System	Apple	Mac Os X	All	All	All	All

Operating System	Apple	Tvos	All	All	All	All
Operating System	Apple	Tvos	All	All	All	All
Operating System	Apple	Watchos	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	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
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 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	6.0	All	All	All
Operating System	Redhat	Enterprise Linux Server	7.0	All	All	All

System						
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 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 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 Server Tus	7.2	All	All	All
Operating	Redhat	Enterprise Linux Server Tus	7.3	All	All	All

System						
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
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
Application	Xmlsoft	Libxml2	All	All	All	All
cpe:2.3:o:apple:iphone_os:*****:						
cpe:2.3:o:apple:iphone_os:*****:						
cpe:2.3:o:apple:mac_os_x:*****:						
cpe:2.3:o:apple:mac_os_x:*****:						
cpe:2.3:o:apple:tvos:*****:						
cpe:2.3:o:apple:tvos:*****:						
cpe:2.3:o:apple:watchos:*****:						
cpe:2.3:o:apple:watchos:*****:						
cpe:2.3:o:canonical:ubuntu_linux:12.04:***:lts:***:						
cpe:2.3:o:canonical:ubuntu_linux:14.04:***:lts:***:						
cpe:2.3:o:canonical:ubuntu_linux:15.10:*****:						
cpe:2.3:o:canonical:ubuntu_linux:16.04:***:lts:***:						
cpe:2.3:o:canonical:ubuntu_linux:12.04:***:lts:***:						
cpe:2.3:o:canonical:ubuntu_linux:14.04:***:lts:***:						
cpe:2.3:o:canonical:ubuntu_linux:15.10:*****:						
cpe:2.3:o:canonical:ubuntu_linux:16.04:***:lts:***:						
cpe:2.3:o:debian:debian_linux:8.0:*****:						
cpe:2.3:o:debian:debian_linux:8.0:*****:						
cpe:2.3:a:mcafee:web_gateway:*****:						
cpe:2.3:a:mcafee:web_gateway:*****:						

```
cpe:2.3:o:redhat:enterprise_linux_desktop:6.0:*:*:*:*:*:*:
```

```
cpe:2.3:o:redhat:enterprise_linux_desktop:7.0:*:*:*:*:*:*
```

```
cpe:2.3:o:redhat:enterprise_linux_desktop:6.0:*:*:*:*:*:*
```

```
cpe:2.3:o:redhat:enterprise_linux_desktop:7.0:*:*:*:*:*:*
```

```
cpe:2.3:o:redhat:enterprise_linux_server:6.0:*:*:*:*:*:*:
```

```
cpe:2.3:o:redhat:enterprise_linux_server:7.0:*:*:*:*:*:*:
```

```
cpe:2.3:o:redhat:enterprise_linux_server:6.0:*:*:*:*:*:*:
```

```
cpe:2.3:o:redhat:enterprise linux server:7.0:*:*:*:*:*:*
```

```
cpe:2.3:o:redhat:enterprise linux server aus:7.2:*:*:*:*:*:
```

```
cpe:2.3:o:redhat:enterprise linux server aus:7.3:*:*:*:*:*:
```

```
cpe:2.3:o:redhat:enterprise_linux_server_aus:7.4.*:*:*:*:*.*
```

```
cpe:2.3:o:redhat:enterprise_linux_server_aus:7.6.*:*:*:*:*.*
```

```
cpe:2.3:o:redhat:enterprise linux server aus:7.2:*:*:*:*:*:
```

```
cpe:2.3:o:redhat:enterprise linux server aus:7.3.*:*:*:*:*:
```

```
cpe:2.3:o:redhat:enterprise linux server aus:7.4.*:*:*:*:*:
```

```
cpe:2.3:o:redhat:enterprise_linux_server_aus:7.6:*:*:*:*:*.*
```

```
cpe:2.3:o:redhat:enterprise_linux_server_eus:7.2:*:*:*:*:*.*
```

```
cpe:2.3:o:redhat:enterprise linux server eus:7.3.*:*:*:*:*.*
```

```
cpe:2.3:o:redhat:enterprise linux server eus:7.4.*:*:*:*:*.*
```

```
cpe:2.3:o:redhat:enterprise linux server eus:7.5:*:*:*:*:*:
```

```
cpe:2.3:o:redhat:enterprise_linux_server_eus:7.6:*:*:*:*:*.*
```

```
cpe:2.3:o:redhat:enterprise linux server eus:7.2:*:*:*:*:*:
```

```
cpe:2.3:o:redhat:enterprise linux server eus:7.3:*:*:*:*:*:
```

```
cpe:2.3:o:redhat:enterprise linux server eus:7.4.*:*:*:*:*:
```

```
cpe:2.3:o:redhat:enterprise linux server eus:7.5:*:*:*:*:*:
```

```
cpe:2.3:o:redhat:enterprise_linux_server_eus:7.6:*:*:*:*:*.*
```

```
cpe:2.3:o:redhat:enterprise linux server tus:7.2:*:*:*:*:*:*
```

```
cpe:2.3:o:redhat:enterprise linux server tus:7.3:*:*:*:*:*:
```

```
one23@redhatenterprise linux ~$ cat /etc/passwd | grep root
```

cpe:2.3:o:redhat:enterprise_linux_server_tus:7.6: : : : : :
cpe:2.3:o:redhat:enterprise_linux_server_tus:7.2: : : : : :
cpe:2.3:o:redhat:enterprise_linux_server_tus:7.3: : : : : :
cpe:2.3:o:redhat:enterprise_linux_server_tus:7.6: : : : : :
cpe:2.3:o:redhat:enterprise_linux_workstation:6.0: : : : : :
cpe:2.3:o:redhat:enterprise_linux_workstation:7.0: : : : : :
cpe:2.3:o:redhat:enterprise_linux_workstation:6.0: : : : : :
cpe:2.3:o:redhat:enterprise_linux_workstation:7.0: : : : : :
cpe:2.3:a:xmlsoft:libxml2: : : : : :
cpe:2.3:a:xmlsoft:libxml2: : : : : :

No vendor comments have been submitted for this CVE

[← Previous ID](#)

Next ID→

© CVE.report 2023   |

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 registered 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](#).

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