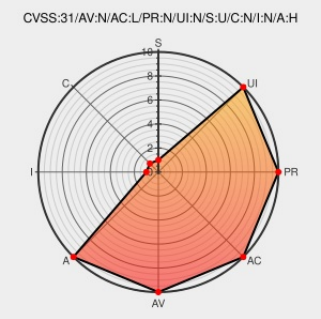
CVE-2022-40303

Published on: Not Yet Published

Last Modified on: 01/11/2023 05:29:00 PM UTC

CVE-2022-40303

Source: Mitre | Source: NIST | CVE.ORG | Print: PDF



Certain versions of Ipados from Apple contain the following vulnerability:

An issue was discovered in libxml2 before 2.10.3. When parsing a multi-gigabyte XML document with the XML_PARSE_HUGE parser option enabled, several integer counters can overflow. This results in an attempt to access an array at a negative 2GB offset, typically leading to a segmentation fault.

CVE-2022-40303 has been assigned by cve@mitre.org to track the vulnerability - currently rated as HIGH severity.

CVSS3 Score: 7.5 - HIGH

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

CVE References

Description	Tags	Link
About the security content of watchOS 9.2 - Apple Support	support.apple.com text/html	CONFIRM support.apple.com/kb/HT213536
About the security content of iOS 15.7.2 and iPadOS 15.7.2 - Apple Support	support.apple.com text/html	CONFIRM support.apple.com/kb/HT213531
About the security content of macOS Big Sur 11.7.2 - Apple Support	support.apple.com text/html	CONFIRM support.apple.com/kb/HT213534
About the security content of macOS Monterey 12.6.2 - Apple Support	support.apple.com text/html	CONFIRM support.apple.com/kb/HT213533
Full Disclosure: APPLE-SA-2022-12-13-2 iOS 15.7.2 and iPadOS 15.7.2	seclists.org text/html	FULLDISC 20221220 APPLE-SA-2022-12-13-2 iOS 15.7.2 and iPadOS 15.7.2
About the security content of tvOS 16.2 - Apple		CONFIRM support.apple.com/kb/HT213535

About the security content of tvOS 16.2 - Apple Support	support.apple.com text/html	CONFIRM support.apple.com/kb/HT213535
Full Disclosure: APPLE-SA-2022-12-13-6 macOS Big Sur 11.7.2	seclists.org text/html	FULLDISC 20221220 APPLE-SA-2022-12-13-6 macOS Big Sur 11.7.2
[CVE-2022-40303] Fix integer overflows with XML_PARSE_HUGE (c8469863) · Commits · GNOME / libxml2 · GitLab	gitlab.gnome.org text/html	MISC gitlab.gnome.org/GNOME/libxml2/-/commit/c846986356fc149915a74972bf198abc266bc2c0
Full Disclosure: APPLE-SA-2022-12-13-5 macOS Monterey 12.6.2	seclists.org text/html	FULLDISC 20221220 APPLE-SA-2022-12-13-5 macOS Monterey 12.6.2
November 2022 Libxml2 Vulnerabilities in NetApp Products | NetApp Product Security	security.netapp.com text/html	CONFIRM security.netapp.com/advisory/ntap-20221209-0003/
v2.10.3 · Tags · GNOME / libxml2 · GitLab	gitlab.gnome.org text/html	MISC gitlab.gnome.org/GNOME/libxml2/-/tags/v2.10.3
No Description Provided	seclists.org Inactive Link Not Archived	FULLDISC 20221220 APPLE-SA-2022-12-13-7 tvOS 16.2
Full Disclosure: APPLE-SA-2022-12-13-8 watchOS 9.2	seclists.org text/html	FULLDISC 20221220 APPLE-SA-2022-12-13-8 watchOS 9.2

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.

Related QID Numbers

160396 Oracle Enterprise Linux Security Update for libxml2 (ELSA-2023-0173)

160413 Oracle Enterprise Linux Security Update for libxml2 (ELSA-2023-0338)

181179 Debian Security Update for libxml2 (DLA 3172-1)

181192 Debian Security Update for libxml2 (DSA 5271-1)

199063 Ubuntu Security Notification for libxml2 Vulnerabilities (USN-5760-1)

241064 Red Hat Update for libxml2 (RHSA-2023:0173)

241093 Red Hat Update for libxml2 (RHSA-2023:0338)

283234 Fedora Security Update for libxml2 (FEDORA-2022-aeafd24818)

283465 Fedora Security Update for libxml2 (FEDORA-2022-a6812b0224)

354430 Amazon Linux Security Advisory for libxml2 : ALAS2022-2022-258

354487 Amazon Linux Security Advisory for xmlsec1 : ALAS2022-2022-257

354559 Amazon Linux Security Advisory for xmlsec1 : ALAS-2022-257

354560 Amazon Linux Security Advisory for libxml2 : ALAS-2022-258

377762 Apple MacOS Ventura 13.0.1 Not Installed (HT213504)

377831 Apple macOS Monterey 12.6.2 Not Installed (HT213533)

377832 Apple macOS Big Sur 11.7.2 Not Installed (HT213534)

377902 Alibaba Cloud Linux Security Update for libxml2 (ALINUX3-SA-2023:0008)

502547 Alpine Linux Security Update for libxml2

610450 Apple iOS 16.1.1 and iPadOS 16.1.1 Security Update Missing

610455 Apple iOS 15.7.2 and iPadOS 15.7.2 Security Update Missing

672422 EulerOS Security Update for libxml2 (EulerOS-SA-2022-2800)

672493 EulerOS Security Update for libxml2 (EulerOS-SA-2023-1016)

672514 EulerOS Security Update for libxml2 (EulerOS-SA-2023-1041)

672550 EulerOS Security Update for libxml2 (EulerOS-SA-2023-1130)

672571 EulerOS Security Update for libxml2 (EulerOS-SA-2023-1106)

710675 Gentoo Linux libxml2 Multiple Vulnerabilities (GLSA 202210-39)

752695 SUSE Enterprise Linux Security Update for libxml2 (SUSE-SU-2022:3692-1)

752722 SUSE Enterprise Linux Security Update for libxml2 (SUSE-SU-2022:3717-1)

752764 SUSE Enterprise Linux Security Update for libxml2 (SUSE-SU-2022:3871-1)

904558 Common Base Linux Mariner (CBL-Mariner) Security Update for libxml2 (11474)

904562 Common Base Linux Mariner (CBL-Mariner) Security Update for libxml2 (11471)

904624 Common Base Linux Mariner (CBL-Mariner) Security Update for libxml2 (11474-1)

904644 Common Base Linux Mariner (CBL-Mariner) Security Update for libxml2 (11471-1)

940884 AlmaLinux Security Update for libxml2 (ALSA-2023:0173)

940901 AlmaLinux Security Update for libxml2 (ALSA-2023:0338)

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Apple	Ipados	All	All	All	All
Operating System	Apple	Iphone Os	All	All	All	All
Operating System	Apple	Macos	All	All	All	All
Operating System	Apple	Tvos	All	All	All	All
Operating System	Apple	Watchos	All	All	All	All
Application	Netapp	Active Iq Unified Manager	-	All	All	All
Application	Netapp	Active Iq Unified Manager For Vmware Vsphere	-	All	All	All
Application	Netapp	Clustered Data Ontap	-	All	All	All
Application	Netapp	Clustered Data Ontap Antivirus Connector	-	All	All	All
Hardware	Netapp	H300s	-	All	All	All

Operating System	Netapp	H300s Firmware	-	All	All	All
Hardware	Netapp	H410c	-	All	All	All
Operating System	Netapp	H410c Firmware	-	All	All	All
Hardware	Netapp	H410s	-	All	All	All
Operating System	Netapp	H410s Firmware	-	All	All	All
Hardware	Netapp	H500s	-	All	All	All
Operating System	Netapp	H500s Firmware	-	All	All	All
Hardware	Netapp	H700s	-	All	All	All
Operating System	Netapp	H700s Firmware	-	All	All	All
Application	Netapp	Netapp Manageability Sdk	-	All	All	All
Application	Netapp	Ontap Select Deploy Administration Utility	-	All	All	All
Application	Netapp	Snapmanager	-	All	All	All
Application	Xmlsoft	Libxml2	All	All	All	All

cpe:2.3:o:apple:ipados:*:*:*:*:*:*:*:*:

cpe:2.3:o:apple:iphone_os:*:*:*:*:*:*:*:*:

cpe:2.3:o:apple:macos:*:*:*:*:*:*:*:*:

cpe:2.3:o:apple:tvos:*:*:*:*:*:*:*:*:

cpe:2.3:o:apple:watchos:*:*:*:*:*:*:*:*:

cpe:2.3:a:netapp:active_iq_unified_manager:-:*:*:*:*:vsphere:*:*:

cpe:2.3:a:netapp:active_iq_unified_manager_for_vmware_vsphere:-:*:*:*:*:*:*:*:

cpe:2.3:a:netapp:clustered_data_ontap:-:*:*:*:*:*:*:*:

cpe:2.3:a:netapp:clustered_data_ontap_antivirus_connector:-:*:*:*:*:*:*:*:

cpe:2.3:h:netapp:h300s:-:*:*:*:*:*:*:*:

cpe:2.3:o:netapp:h300s_firmware:-:*:*:*:*:*:*:*:

cpe:2.3:h:netapp:h410c:-:*:*:*:*:*:*:*:

cpe:2.3:o:netapp:h410c_firmware:-:*:*:*:*:*:*:*:

cpe:2.3:h:netapp:h410s:-:*:*:*:*:*:*:*:

cpe:2.3:o:netapp:h410s_firmware:-:*:*:*:*:*:*:*:

cpe:2.3:h:netapp:h500s:-:*:*:*:*:*:*:*:

cpe:2.3:o:netapp:h500s_firmware:-:*:*:*:*:*:*:*:

cpe:2.3:h:netapp:h700s:-:*:*:*:*:*:*:*:

cpe:2.3:o:netapp:h700s_firmware:-:*:*:*:*:*:*:*:

cpe:2.3:a:netapp:netapp_manageability_sdk:-:*:*:*:*:*:*:*:

cpe:2.3:a:netapp:ontap_select_deploy_administration_utility:-:*:*:*:*:*:*:*:

cpe:2.3:a:netapp:snapmanager:-:*:*:*:*:hyper-v:*:*:

cpe:2.3:a:xmlsoft:libxml2:*:*:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

Social Mentions

Source	Title	Posted (UTC)
@vigilance_fr	Vigil@nce #Vulnérabilité de libxml2 : trois vulnérabilités. vigilance.fr/vulnerabilite/… Références : #CVE-2022-40303,… twitter.com/i/web/status/1…	2022-10-15 09:09:03
@vigilance_en	Vigil@nce #Vulnerability of libxml2: three vulnerabilities. vigilance.fr/vulnerability/… Identifiers: #CVE-2022-40303,… twitter.com/i/web/status/1…	2022-10-15 09:09:04
@autumn_good_35	CVE-2022-37434 CVE-2022-40303 CVE-2022-40304 ClamAV® blog: New packages for ClamAV 0.103.7, 0.104.4, 0.105.1 to res… twitter.com/i/web/status/1…	2022-11-01 15:09:30
@_r_netsec	Integer overflow in xmlParseNameComplex (libxml2) - CVE-2022-40303 gitlab.gnome.org/GNOME/libxml2/…	2022-11-10 01:28:07
@luiscosio	Desbordamiento de enteros en xmlParseNameComplex (libxml2) - CVE-2022-40303 - zpr.io/CuwsJjG5sDrU #NETSEC	2022-11-10 01:34:27
@Myinfosecfeed	New post: "Integer overflow in xmlParseNameComplex (libxml2) - CVE-2022-40303" ift.tt/mNdY86B	2022-11-10 01:48:40
@CybrXx0	Integer overflow in xmlParseNameComplex (libxml2) - CVE-2022-40303 via /r/netsec ift.tt/ZJqONWs #cybersecurity #netsec #news	2022-11-10 01:59:13
@olouhaidia	Integer overflow in xmlParseNameComplex (libxml2) - CVE-2022-40303 bit.ly/3tmREq8	2022-11-10 02:29:56
@0xdea	[CVE-2022-40303] Integer overflow in xmlParseNameComplex // by @maddiestone gitlab.gnome.org/GNOME/libxml2/…	2022-11-10 06:05:40
@ksg93rd	#exploit 1. CVE-2022-40303: Integer overflow in xmlParseNameComplex gitlab.gnome.org/GNOME/libxml2/…	2022-11-10 12:48:12
@the_yellow_fall	CVE-2022-40303 & CVE-2022-40304: RCE flaws in Apple iOS, macOS securityonline.info/cve-2022-40303… #opensource #infosec #security #pentesting	2022-11-11 06:54:54
@AcooEdi	CVE-2022-40303 & CVE-2022-40304: RCE flaws in Apple iOS, macOS dlvr.it/ScbFD0 via securityonline https://t.co/pn5R9O4Aoy	2022-11-11 06:58:35
@lucianot54	"CVE-2022-40303 & CVE-2022-40304: RCE flaws in Apple iOS, macOS" via Penetration Testing ift.tt/6pKoB2S	2022-11-11 07:17:18
@FilipiPires	CVE-2022-40303 & CVE-2022-40304: RCE flaws in Apple iOS, macOS ift.tt/q1FI2sD #security	2022-11-11

	#opensource… twitter.com/i/web/status/1…	07:33:40
@Dinosn	CVE-2022-40303 & CVE-2022-40304: RCE flaws in Apple iOS, macOS securityonline.info/cve-2022-40303…	2022-11-11 07:40:09
@Komodosec	#Vulnerability #Apple CVE-2022-40303 & CVE-2022-40304: RCE flaws in Apple iOS, macOS securityonline.info/cve-2022-40303…	2022-11-11 11:05:32
@PentestingN	CVE-2022-40303 & CVE-2022-40304: RCE flaws in Apple iOS, macOS securityonline.info/cve-2022-40303… Penetration Testing CVE-20… twitter.com/i/web/status/1…	2022-11-11 11:13:43
@ernered	CVE-2022-40303 & CVE-2022-40304: RCE flaws in Apple iOS, macOS securityonline.info/cve-2022-40303… #technology #feedly	2022-11-13 16:05:38
@hagieee	iOS/iPadOS 1.6.1.1リリース libxml2の脆弱性(CVE-2022-40303, CVE-2022-40304) 2件が修正 support.apple.com/ja-jp/HT213505	2022-11-14 04:48:10
@iototsecnews	macOS / iOS のリモート・コード実行の脆弱性が FIX：CVE-2022-40303 / CVE-2022-40304 #security #apple #vulnerability iototsecnews.jp/2022/11/10/app…	2022-11-19 22:08:46
@CVEreport	CVE-2022-40303 : An issue was discovered in libxml2 before 2.10.3. When parsing a multi-gigabyte XML document with… twitter.com/i/web/status/1…	2022-11-23 00:08:41
@ColorTokensInc	Emerging Vulnerability Found CVE-2022-40303 - An issue was discovered in libxml2 before 2.10.3. When parsing a mult… twitter.com/i/web/status/1…	2022-11-23 00:26:57
/r/netsec	Integer overflow in xmlParseNameComplex (libxml2) - CVE-2022-40303	2022-11-10 01:24:29
/r/k12cybersecurity	MS-ISAC CYBERSECURITY ADVISORY - Multiple Vulnerabilities in Apple Products Could Allow for Arbitrary Code Execution - PATCH: NOW	2022-11-10 12:55:52
/r/netcve	CVE-2022-40303	2022-11-23 01:39:02
/r/cybersecurity	macOS Monterey still vulnerable to CVE-2022-40303	2022-12-01 19:23:17
/r/MacOS	macOS Monterey still vulnerable to CVE-2022-40303	2022-12-01 19:22:57
/r/mac	macOS Monterey still vulnerable to CVE-2022-40303	2022-12-01 19:22:55
/r/hypeurls	macOS Monterey still vulnerable to CVE-2022-40303	2022-12-03 19:06:37
/r/k12cybersecurity	MS-ISAC CYBERSECURITY ADVISORY - Multiple Vulnerabilities in Apple Products Could Allow for Arbitrary Code Execution - PATCH: NOW	2022-12-14 15:20:38

← 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 registred 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