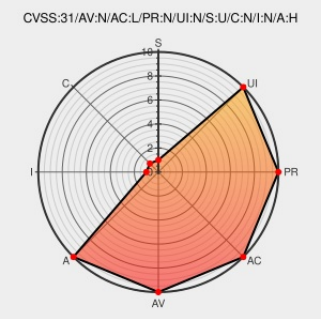
CVE-2022-23308

Published on: Not Yet Published

Last Modified on: 11/02/2022 01:18:00 PM UTC

CVE-2022-23308

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



Certain versions of Ipados from Apple contain the following vulnerability:

valid.c in libxml2 before 2.9.13 has a use-after-free of ID and IDREF attributes.

CVE-2022-23308 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

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
libxml2: Multiple Vulnerabilities (GLSA 202210-03) — Gentoo security	security.gentoo.org text/html	GENTOO GLSA-202210-03

About the security content of iOS 15.5 and iPadOS 15.5 - Apple Support	support.apple.com text/html	CONFIRM support.apple.com/kb/HT213258
About the security content of macOS Big Sur 11.6.6 - Apple Support	support.apple.com text/html	CONFIRM support.apple.com/kb/HT213256
Full Disclosure: APPLE-SA-2022-05-16-2 macOS Monterey 12.4	seclists.org text/html	FULLDISC 20220516 APPLE-SA-2022-05-16-2 macOS Monterey 12.4
About the security content of macOS Monterey 12.4 - Apple Support	support.apple.com text/html	CONFIRM support.apple.com/kb/HT213257
CVE-2022-23308 Libxml2 Vulnerability in NetApp Products | NetApp Product Security	security.netapp.com text/html	CONFIRM security.netapp.com/advisory/ntap-20220331-0008/
[SECURITY] [DLA 2972-1] libxml2 security update	lists.debian.org text/html	MLIST [debian-lts-announce] 20220408 [SECURITY] [DLA 2972-1] libxml2 security update
[SECURITY] Fedora 34 Update: libxml2-2.9.13-1.fc34 - package-announce - Fedora Mailing-Lists	lists.fedoraproject.org text/html	FEDORA FEDORA-2022-050c712ed7
NEWS · v2.9.13 · GNOME / libxml2 · GitLab	gitlab.gnome.org text/html	MISC gitlab.gnome.org/GNOME/libxml2/-/blob/v2.9.13/NEWS
Full Disclosure: APPLE-SA-2022-05-16-5 watchOS 8.6	seclists.org text/html	FULLDISC 20220516 APPLE-SA-2022-05-16-5 watchOS 8.6
About the security content of Security Update 2022-004 Catalina - Apple Support	support.apple.com text/html	CONFIRM support.apple.com/kb/HT213255
About the security content of watchOS 8.6 - Apple Support	support.apple.com text/html	CONFIRM support.apple.com/kb/HT213253
Full Disclosure: APPLE-SA-2022-05-16-6 tvOS 15.5	seclists.org text/html	FULLDISC 20220516 APPLE-SA-2022-05-16-6 tvOS 15.5
About the security content of tvOS 15.5 - Apple Support	support.apple.com text/html	CONFIRM support.apple.com/kb/HT213254
Full Disclosure: APPLE-SA-2022-05-16-1 iOS 15.5 and iPadOS 15.5	seclists.org text/html	FULLDISC 20220516 APPLE-SA-2022-05-16-1 iOS 15.5 and iPadOS 15.5
Full Disclosure: APPLE-SA-2022-05-16-3 macOS Big Sur 11.6.6	seclists.org text/html	FULLDISC 20220516 APPLE-SA-2022-05-16-3 macOS Big Sur 11.6.6
[CVE-2022-23308] Use-after-free of ID and IDREF attributes · GNOME/libxml2@652dd12 · GitHub	github.com text/html	CONFIRM github.com/GNOME/libxml2/commit/652dd12a858989b14eed4e84e453059cd3ba340e
Full Disclosure: APPLE-	seclists.org	FULLDISC 20220516 APPLE-SA-2022-05-16-4 Security Update 2022-004 Catalina

SA-2022-05-16-4 Security Update 2022-004 Catalina	text/html	
Oracle Critical Patch Update Advisory - July 2022	www.oracle.com text/html	MISC www.oracle.com/security-alerts/cpujul2022.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.

Related QID Numbers

159707 Oracle Enterprise Linux Security Update for libxml2 (ELSA-2022-0899)

179176 Debian Security Update for libxml2 (DLA 2972-1)

179208 Debian Security Update for libxml2 (CVE-2022-23308)

198697 Ubuntu Security Notification for libxml2 Vulnerability (USN-5324-1)

198787 Ubuntu Security Notification for libxml2 Vulnerabilities (USN-5422-1)

240152 Red Hat Update for libxml2 (RHSA-2022:0899)

240235 Red Hat Update for JBoss Core Services (RHSA-2022:1389)

282425 Fedora Security Update for libxml2 (FEDORA-2022-b661dea83d)

282462 Fedora Security Update for libxml2 (FEDORA-2022-050c712ed7)

296063 Oracle Solaris 11.4 Support Repository Update (SRU) 45.119.2 Missing (CPUAPR2022)

354006 Amazon Linux Security Advisory for libxml2 : ALAS2-2022-1826

354464 Amazon Linux Security Advisory for libxml2 : ALAS2022-2022-198

354486 Amazon Linux Security Advisory for libxml2 : ALAS2022-2022-068

354638 Amazon Linux Security Advisory for libxml2 : AL2012-2022-370

354929 Amazon Linux Security Advisory for libxml2 : ALAS-2023-1743

355209 Amazon Linux Security Advisory for libxml2 : ALAS2023-2023-096

376607 Apple macOS Security Update 2022-004 Catalina (HT213255)

376608 Apple MacOS Big Sur 11.6.6 Not Installed (HT213256)

376612 Apple macOS Monterey 12.4 Not Installed (HT213257)

377365 Alibaba Cloud Linux Security Update for libxml2 (ALINUX3-SA-2022:0018)

377726 F5 BIG-IP Libxml2 vulnerability cve-2022-23308 (K32760744)

377937 Splunk Enterprise Multiple Vulnerabilities (svd-2022-0804)

500344 Alpine Linux Security Update for libxml2

502932 Alpine Linux Security Update for qt5-qtwebengine

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

610416 Apple iOS 15.5 and iPadOS 15.5 Security Update Missing (HT213258)

671562 EulerOS Security Update for libxml2 (EulerOS-SA-2022-1574)

671602 EulerOS Security Update for libxml2 (EulerOS-SA-2022-1541)

671675 EulerOS Security Update for libxml2 (EulerOS-SA-2022-1741)

671744 EulerOS Security Update for libxml2 (EulerOS-SA-2022-1810)

671750 EulerOS Security Update for libxml2 (EulerOS-SA-2022-1793)

671794 EulerOS Security Update for libxml2 (EulerOS-SA-2022-1870)

671803 EulerOS Security Update for libxml2 (EulerOS-SA-2022-1846)

710642 Gentoo Linux libxml2 Multiple Vulnerabilities (GLSA 202210-03)

751855 SUSE Enterprise Linux Security Update for python-libxml2-python (SUSE-SU-2022:0802-1)

751859 OpenSUSE Security Update for python-libxml2-python (openSUSE-SU-2022:0802-1)

752068 SUSE Enterprise Linux Security Update for libxml2 (SUSE-SU-2022:1308-1)

752156 SUSE Enterprise Linux Security Update for libxml2 (SUSE-SU-2022:1750-1)

752389 SUSE Enterprise Linux Security Update for libxml2 (SUSE-SU-2022:2552-1)

753147 SUSE Enterprise Linux Security Update for libxml2 (SUSE-SU-2022:14904-1)

900725 Common Base Linux Mariner (CBL-Mariner) Security Update for libxml2 (8851)

901008 Common Base Linux Mariner (CBL-Mariner) Security Update for libxml2 (8862-1)

940468 AlmaLinux Security Update for libxml2 (ALSA-2022:0899)

960820 Rocky Linux Security Update for libxml2 (RLSA-2022:0899)

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	Macos	10.15.7	All	All	All
Operating System	Apple	Macos	10.15.7	security_update_2020-001	All	All
Operating System	Apple	Macos	10.15.7	security_update_2021-001	All	All
Operating System	Apple	Macos	10.15.7	security_update_2021-002	All	All
Operating System	Apple	Macos	10.15.7	security_update_2021-003	All	All

Operating System	Apple	Macos	10.15.7	security_update_2021-004	All	All
Operating System	Apple	Macos	10.15.7	security_update_2021-005	All	All
Operating System	Apple	Macos	10.15.7	security_update_2021-006	All	All
Operating System	Apple	Macos	10.15.7	security_update_2021-007	All	All
Operating System	Apple	Macos	10.15.7	security_update_2021-008	All	All
Operating System	Apple	Macos	10.15.7	security_update_2022-001	All	All
Operating System	Apple	Macos	10.15.7	security_update_2022-003	All	All
Operating System	Apple	Mac Os X	All	All	All	All
Operating System	Apple	Mac Os X	10.15.7	All	All	All
Operating System	Apple	Mac Os X	10.15.7	security_update_2020-001	All	All
Operating System	Apple	Mac Os X	10.15.7	security_update_2021-001	All	All
Operating System	Apple	Mac Os X	10.15.7	security_update_2021-002	All	All
Operating System	Apple	Mac Os X	10.15.7	security_update_2021-003	All	All
Operating System	Apple	Mac Os X	10.15.7	security_update_2021-004	All	All
Operating System	Apple	Mac Os X	10.15.7	security_update_2021-005	All	All
Operating System	Apple	Mac Os X	10.15.7	security_update_2021-006	All	All
Operating System	Apple	Mac Os X	10.15.7	security_update_2021-007	All	All
Operating System	Apple	Mac Os X	10.15.7	security_update_2021-008	All	All
Operating System	Apple	Mac Os X	10.15.7	security_update_2022-001	All	All
Operating System	Apple	Mac Os X	10.15.7	security_update_2022-003	All	All
Operating System	Apple	Tvos	All	All	All	All
Operating System	Apple	Watchos	All	All	All	All
Operating System	Debian	Debian Linux	9.0	All	All	All

Operating System	Fedoraproject	Fedora	34	All	All	All
Application	Netapp	Active Iq Unified Manager	-	All	All	All
Operating System	Netapp	Bootstrap Os	-	All	All	All
Application	Netapp	Clustered Data Ontap	-	All	All	All
Application	Netapp	Clustered Data Ontap Antivirus Connector	-	All	All	All
Hardware	Netapp	H300e	-	All	All	All
Operating System	Netapp	H300e Firmware	-	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	H500e	-	All	All	All
Operating System	Netapp	H500e Firmware	-	All	All	All
Hardware	Netapp	H500s	-	All	All	All
Operating System	Netapp	H500s Firmware	-	All	All	All
Hardware	Netapp	H700e	-	All	All	All
Operating System	Netapp	H700e Firmware	-	All	All	All
Hardware	Netapp	H700s	-	All	All	All
Operating System	Netapp	H700s Firmware	-	All	All	All
Hardware	Netapp	Hci Compute Node	-	All	All	All
Application	Netapp	Manageability Software Development Kit	-	All	All	All
Application	Netapp	Ontap Select Deploy Administration Utility	-	All	All	All

Application	Netapp	Ontap Select Deploy Administration Utility	-	All	All	All
Application	Netapp	Smi-s Provider	-	All	All	All
Application	Netapp	Snapdrive	-	All	All	All
Application	Netapp	Snapmanager	-	All	All	All
Application	Netapp	Solidfire Enterprise Sds Hci Storage Node	-	All	All	All
Application	Netapp	Solidfire Hci Management Node	-	All	All	All
Application	Oracle	Communications Cloud Native Core Binding Support Function	22.2.0	All	All	All
Application	Oracle	Communications Cloud Native Core Network Function Cloud Native Environment	22.1.0	All	All	All
Application	Oracle	Communications Cloud Native Core Network Repository Function	22.1.2	All	All	All
Application	Oracle	Communications Cloud Native Core Network Repository Function	22.2.0	All	All	All
Application	Oracle	Communications Cloud Native Core Network Slice Selection Function	22.1.1	All	All	All
Application	Oracle	Communications Cloud Native Core Unified Data Repository	22.2.0	All	All	All
Application	Oracle	Mysql Workbench	All	All	All	All
Application	Oracle	Zfs Storage Appliance Kit	8.8	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:macos:10.15.7:*:*:*:*:*:*:*:

cpe:2.3:o:apple:macos:10.15.7:security_update_2020-001:*:*:*:*:*:*:

cpe:2.3:o:apple:macos:10.15.7:security_update_2021-001:*:*:*:*:*:*:

cpe:2.3:o:apple:macos:10.15.7:security_update_2021-002:*:*:*:*:*:*:

cpe:2.3:o:apple:macos:10.15.7:security_update_2021-003:*:*:*:*:*:*:

cpe:2.3:o:apple:macos:10.15.7:security_update_2021-004:*:*:*:*:*:*:

cpe:2.3:o:apple:macos:10.15.7:security_update_2021-005:*:*:*:*:*:*:

cpe:2.3:o:apple:macos:10.15.7:security_update_2021-006:*:*:*:*:*:*:

cpe:2.3:o:apple:macos:10.15.7:security_update_2021-007:*:*:*:*:*:*:

cpe:2.3:o:apple:macos:10.15.7:security_update_2021-008:*:*:*:*:*:*:

cpe:2.3:o:apple:macos:10.15.7:security_update_2022-001:*:*:*:*:*:*:

cpe:2.3:o:apple:macos:10.15.7:security_update_2022-003:*:*:*:*:*:*:*:

cpe:2.3:o:apple:mac_os_x:*:*:*:*:*:*:*:*:

cpe:2.3:o:apple:mac_os_x:10.15.7:*:*:*:*:*:*:*:

cpe:2.3:o:apple:mac_os_x:10.15.7:security_update_2020-001:*:*:*:*:*:*:

cpe:2.3:o:apple:mac_os_x:10.15.7:security_update_2021-001:*:*:*:*:*:*:

cpe:2.3:o:apple:mac_os_x:10.15.7:security_update_2021-002:*:*:*:*:*:*:

cpe:2.3:o:apple:mac_os_x:10.15.7:security_update_2021-003:*:*:*:*:*:*:

cpe:2.3:o:apple:mac_os_x:10.15.7:security_update_2021-004:*:*:*:*:*:*:

cpe:2.3:o:apple:mac_os_x:10.15.7:security_update_2021-005:*:*:*:*:*:*:

cpe:2.3:o:apple:mac_os_x:10.15.7:security_update_2021-006:*:*:*:*:*:*:

cpe:2.3:o:apple:mac_os_x:10.15.7:security_update_2021-007:*:*:*:*:*:*:

cpe:2.3:o:apple:mac_os_x:10.15.7:security_update_2021-008:*:*:*:*:*:*:

cpe:2.3:o:apple:mac_os_x:10.15.7:security_update_2022-001:*:*:*:*:*:*:

cpe:2.3:o:apple:mac_os_x:10.15.7:security_update_2022-003:*:*:*:*:*:*:

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

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

cpe:2.3:o:debian:debian_linux:9.0:*:*:*:*:*:*:*:

cpe:2.3:o:fedoraproject:fedora:34:*:*:*:*:*:*:*:

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

cpe:2.3:o:netapp:bootstrap_os:-:*:*:*:*:*:*:*:

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

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

cpe:2.3:h:netapp:h300e:-:*:*:*:*:*:*:*:

cpe:2.3:o:netapp:h300e_firmware:-:*:*:*:*:*:*:*:

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:h500e:-:*:*:*:*:*:*:*:

cpe:2.3:o:netapp:h500e_firmware:-:*:*:*:*:*:*:*:

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

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

cpe:2.3:h:netapp:h700e:-:*:*:*:*:*:*:*:

cpe:2.3:o:netapp:h700e_firmware:-:*:*:*:*:*:*:*:

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

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

cpe:2.3:h:netapp:hci_compute_node:-:*:*:*:*:*:*:*:

cpe:2.3:a:netapp:manageability_software_development_kit:-:*:*:*:*:*:*:*:

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

cpe:2.3:a:netapp:smi-s_provider:-:*:*:*:*:*:*:*:

cpe:2.3:a:netapp:snapdrive:-:*:*:*:*:unix:*:*:

cpe:2.3:a:netapp:snapmanager:-:*:*:*:*:oracle:*:*:

cpe:2.3:a:netapp:solidfire\,_enterprise_sds_\&_hci_storage_node:-:*:*:*:*:*:*:*:

cpe:2.3:a:netapp:solidfire_\&_hci_management_node:-:*:*:*:*:*:*:*:

cpe:2.3:a:oracle:communications_cloud_native_core_binding_support_function:22.2.0:*:*:*:*:*:*:*:

cpe:2.3:a:oracle:communications_cloud_native_core_network_function_cloud_native_environment:22.1.0:*:*:*:*:*:*:*:

cpe:2.3:a:oracle:communications_cloud_native_core_network_repository_function:22.1.2:*:*:*:*:*:*:*:

cpe:2.3:a:oracle:communications_cloud_native_core_network_repository_function:22.2.0:*:*:*:*:*:*:*:

cpe:2.3:a:oracle:communications_cloud_native_core_network_slice_selection_function:22.1.1:*:*:*:*:*:*:*:

cpe:2.3:a:oracle:communications_cloud_native_core_unified_data_repository:22.2.0:*:*:*:*:*:*:*:

cpe:2.3:a:oracle:mysql_workbench:*:*:*:*:*:*:*:*:

cpe:2.3:a:oracle:zfs_storage_appliance_kit:8.8:*:*:*:*:*:*:*:

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

No vendor comments have been submitted for this CVE

Social Mentions

Source	Title	Posted (UTC)
@CVEreport	CVE-2022-23308 : valid.c in libxml2 before 2.9.13 has a use-after-free of ID and IDREF attributes.... cve.report/CVE-2022-23308	2022-02-28 18:56:58
@RemotelyAlerts	Severity: ?? | valid.c in libxml2 before 2.9.13 has a u... | CVE-2022-23308 | Link for more: alerts.remotelyrmm.com/CVE-2022-23308	2022-03-08 20:02:13
/r/NETGEAR	New - Voxel Custom firmware build for R9000/R8900 v. 1.0.4.59HF Released	2022-04-05 15:08:16
/r/NETGEAR	New - Voxel Custom Firmware build for R7800 v. 1.0.2.93SF Released	2022-04-05 15:03:11
/r/k12cybersecurity	MS-ISAC CYBERSECURITY ADVISORY - Multiple Vulnerabilities in Apple Products Could Allow for Arbitrary Code Execution - PATCH: NOW	2022-05-17 13:11:14
/r/k12cybersecurity	UPDATED MS-ISAC CYBERSECURITY ADVISORY - Multiple Vulnerabilities in Apple Products Could Allow for Arbitrary Code Execution - PATCH: NOW	2022-05-18 14:59:44
/r/synology	DSM Version: 7.2-64561	2023-05-22 03:16:44

← 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