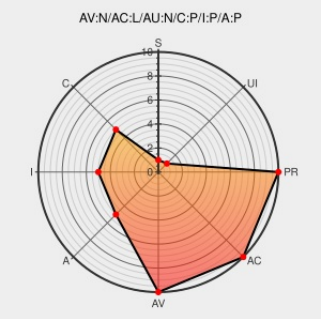
CVE-2010-4494

Published on: 12/07/2010 12:00:00 AM UTC

Last Modified on: 03/25/2021 11:02:30 PM UTC

CVE-2010-4494

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



Certain versions of Openoffice from Apache contain the following vulnerability:

Double free vulnerability in libxml2 2.7.8 and other versions, as used in Google Chrome before 8.0.552.215 and other products, allows remote attackers to cause a denial of service or possibly have unspecified other impact via vectors related to XPath handling.

CVE-2010-4494 has been assigned by cve@mitre.org to track the vulnerability

CVSS2 Score: 7.5 - HIGH

Access Vector	Access Complexity	Authentication
NETWORK	LOW	NONE
Confidentiality Impact	**Integrity Impact**	**Availability Impact**
PARTIAL	PARTIAL	PARTIAL

CVE References

Description	Tags	Link
APPLE-SA-2011-03-21-1 Mac OS X v10.6.7 and Security Update 2011-001	Mailing List, Third Party Advisory, lists.apple.com, text/html	APPLE APPLE-SA-2011-03-21-1
APPLE-SA-2011-03-09-1 iOS 4.3	Mailing List, Third Party Advisory, lists.apple.com, text/html	APPLE APPLE-SA-2011-03-09-1
About the security content of Safari 5.0.4	Broken Link, web.archive.org, text/html, Inactive Link, Not Archived	CONFIRM support.apple.com/kb/HT4566
CVE-2010-4008	Third Party Advisory, www.openoffice.org	CONFIRM www.openoffice.org/security/cves/CVE-2010-

	text/html	4008_CVE-2010-4494.html
Debian update for libxml2 - Advisories - Community	Third Party Advisory web.archive.org text/html	SECUNIA 42762
[SECURITY] Fedora 14 Update: libxml2-2.7.7-3.fc14	Third Party Advisory lists.fedoraproject.org text/html	FEDORA FEDORA-2011-2697
Webmail : Solution de messagerie professionnelle - OVHcloud- OVH	Third Party Advisory www.vupen.com text/html	VUPEN ADV-2010-3336
Support	Third Party Advisory www.redhat.com text/html	REDHAT RHSA-2011:1749
OpenOffice.org Multiple Vulnerabilities - Advisories - Community	Third Party Advisory web.archive.org text/html	SECUNIA 40775
Libxml2 XPath Double Free Vulnerability - Advisories - Community	Third Party Advisory web.archive.org text/html	SECUNIA 42721
About the security content of iTunes 10.2 - Apple Support	Third Party Advisory support.apple.com text/html	CONFIRM support.apple.com/kb/HT4554
APPLE-SA-2011-03-09-2 Safari 5.0.4	Mailing List Third Party Advisory lists.apple.com text/html	APPLE APPLE-SA-2011-03-09-2
Google Chrome Releases: Stable, Beta Channel Updates	Vendor Advisory googlechromereleases.blogspot.com text/html	CONFIRM googlechromereleases.blogspot.com/2010/12/stable-beta-channel-updates.html
Red Hat Customer Portal	Third Party Advisory web.archive.org text/html Inactive Link Not Archived	REDHAT RHSA-2013:0217
Google Chrome Multiple Vulnerabilities - Advisories - Community	Third Party Advisory web.archive.org text/html	SECUNIA 42472
'[security bulletin] HPSBGN02970 rev.1 - HP Rapid Deployment Pack (RDP) or HP Insight Control Server ' - MARC	Third Party Advisory marc.info text/html	HP HPSBGN02970
Support / Security / Advisories / / MDVSA-2010:260 | Mandriva	Third Party Advisory www.mandriva.com text/html	MANDRIVA MDVSA-2010:260
Webmail : Solution de messagerie professionnelle - OVHcloud- OVH	Third Party Advisory www.vupen.com text/html	VUPEN ADV-2010-3319
About the security content of Mac OS X v10.6.7 and Security Update 2011-001	Third Party Advisory support.apple.com text/html	CONFIRM support.apple.com/kb/HT4581
Debian -- Security Information -- DSA-2137-1 libxml2	Third Party Advisory www.debian.org Depreciated Link	DEBIAN DSA-2137

	text/html	
Repository / Oval Repository	Third Party Advisory oval.cisecurity.org text/html	OVAL oval:org.mitre.oval:def:11916
63444 - chromium - An open-source project to help move the web forward. - Monorail	Exploit Issue Tracking Patch Vendor Advisory code.google.com text/html	CONFIRM code.google.com/p/chromium/issues/detail?id=63444
About the security content of iOS 4.3	Third Party Advisory support.apple.com text/html	CONFIRM support.apple.com/kb/HT4564
APPLE-SA-2011-03-02-1 iTunes 10.2	Mailing List Third Party Advisory lists.apple.com text/html	APPLE APPLE-SA-2011-03-02-1
[security-announce] SUSE Security Summary Report: SUSE-SR:2011:005	Third Party Advisory lists.opensuse.org text/html	SUSE SUSE-SR:2011:005
Webmail : Solution de messagerie professionnelle - OVHcloud- OVH	Third Party Advisory www.vupen.com text/html	VUPEN ADV-2011-0230

There are currently no QIDs associated with this CVE

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Apache	Openoffice	All	All	All	All
Application	Apache	Openoffice	All	All	All	All
Application	Apache	Openoffice	All	All	All	All
Operating System	Apple	Iphone Os	All	All	All	All
Operating System	Apple	Iphone Os	All	All	All	All
Application	Apple	Itunes	All	All	All	All
Application	Apple	Itunes	All	All	All	All
Operating System	Apple	Mac Os X	All	All	All	All
Operating System	Apple	Mac Os X	All	All	All	All
Application	Apple	Safari	All	All	All	All

Application	Apple	Safari	All	All	All	All
Operating System	Debian	Debian Linux	5.0	All	All	All
Operating System	Debian	Debian Linux	6.0	All	All	All
Operating System	Debian	Debian Linux	5.0	All	All	All
Operating System	Debian	Debian Linux	6.0	All	All	All
Operating System	Fedoraproject	Fedora	14	All	All	All
Operating System	Fedoraproject	Fedora	14	All	All	All
Application	Google	Chrome	All	All	All	All
Application	Google	Chrome	All	All	All	All
Application	Hp	Insight Control Server Deployment	All	All	All	All
Application	Hp	Insight Control Server Deployment	All	All	All	All
Application	Hp	Rapid Deployment Pack	All	All	All	All
Application	Hp	Rapid Deployment Pack	All	All	All	All
Operating System	Opensuse	Opensuse	11.2	All	All	All
Operating System	Opensuse	Opensuse	11.3	All	All	All
Operating System	Opensuse	Opensuse	11.2	All	All	All
Operating System	Opensuse	Opensuse	11.3	All	All	All
Operating System	Redhat	Enterprise Linux Desktop	6.0	All	All	All
Operating System	Redhat	Enterprise Linux Desktop	6.0	All	All	All
Operating System	Redhat	Enterprise Linux Eus	6.3	All	All	All
Operating System	Redhat	Enterprise Linux Eus	6.3	All	All	All
Operating System	Redhat	Enterprise Linux Server	6.0	All	All	All
Operating System	Redhat	Enterprise Linux Server	6.0	All	All	All
Operating System	Redhat	Enterprise Linux Workstation	6.0	All	All	All
Operating System	Redhat	Enterprise Linux Workstation	6.0	All	All	All
Operating	Suse	Suse Linux Enterprise Server	11	sp1	All	All

System						
Operating System	Suse	Suse Linux Enterprise Server	11	sp1	All	All
Application	Xmlsoft	Libxml2	All	All	All	All

- cpe:2.3:a:apache:openoffice:*:*:*:*:*:*:*:*:
- cpe:2.3:a:apache:openoffice:*:*:*:*:*:*:*:*:
- cpe:2.3:a:apache:openoffice:*:*:*:*:*:*:*:*:
- cpe:2.3:o:apple:iphone_os:*:*:*:*:*:*:*:*:
- cpe:2.3:o:apple:iphone_os:*:*:*:*:*:*:*:*:
- cpe:2.3:a:apple:itunes:*:*:*:*:*:*:*:*:
- cpe:2.3:a:apple:itunes:*:*:*:*:*:*:*:*:
- cpe:2.3:o:apple:mac_os_x:*:*:*:*:*:*:*:*:
- cpe:2.3:o:apple:mac_os_x:*:*:*:*:*:*:*:*:
- cpe:2.3:a:apple:safari:*:*:*:*:*:*:*:*:
- cpe:2.3:a:apple:safari:*:*:*:*:*:*:*:*:
- cpe:2.3:o:debian:debian_linux:5.0:*:*:*:*:*:*:*:
- cpe:2.3:o:debian:debian_linux:6.0:*:*:*:*:*:*:*:
- cpe:2.3:o:debian:debian_linux:5.0:*:*:*:*:*:*:*:
- cpe:2.3:o:debian:debian_linux:6.0:*:*:*:*:*:*:*:
- cpe:2.3:o:fedoraproject:fedora:14:*:*:*:*:*:*:*:
- cpe:2.3:o:fedoraproject:fedora:14:*:*:*:*:*:*:*:
- cpe:2.3:a:google:chrome:*:*:*:*:*:*:*:*:
- cpe:2.3:a:google:chrome:*:*:*:*:*:*:*:*:
- cpe:2.3:a:hp:insight_control_server_deployment:*:*:*:*:*:*:*:*:
- cpe:2.3:a:hp:insight_control_server_deployment:*:*:*:*:*:*:*:*:
- cpe:2.3:a:hp:rapid_deployment_pack:*:*:*:*:*:*:*:*:
- cpe:2.3:a:hp:rapid_deployment_pack:*:*:*:*:*:*:*:*:
- cpe:2.3:o:opensuse:opensuse:11.2:*:*:*:*:*:*:*:
- cpe:2.3:o:opensuse:opensuse:11.3:*:*:*:*:*:*:*:
- cpe:2.3:o:opensuse:opensuse:11.2:*:*:*:*:*:*:*:

cpe:2.3:o:opensuse:opensuse:11.3:*:*:*:*:*:*:*:

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

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

cpe:2.3:o:redhat:enterprise_linux_eus:6.3:*:*:*:*:*:*:*:

cpe:2.3:o:redhat:enterprise_linux_eus:6.3:*:*:*:*:*:*:*:

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

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

cpe:2.3:o:redhat:enterprise_linux_workstation:6.0:*:*:*:*:*:*:*:

cpe:2.3:o:redhat:enterprise_linux_workstation:6.0:*:*:*:*:*:*:*:

cpe:2.3:o:suse:suse_linux_enterprise_server:11:sp1:*:*:*:*:*:*:

cpe:2.3:o:suse:suse_linux_enterprise_server:11:sp1:*:*:*:*:*:*:

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

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→