



Published on: 04/21/2006 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:25:00 PM UTC

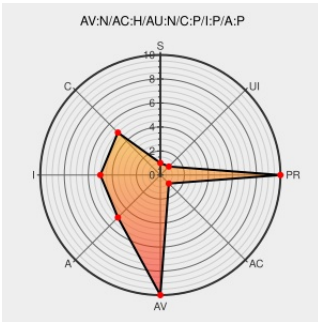
CVE-2006-1985

Source: Mitre

Source: NIST

CVE.ORG

Print: PDF



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

Heap-based buffer overflow in BOM BOMArchiveHelper 10.4 (6.3) Build 312, as used in Mac OS X 10.4.6 and earlier, allows user-assisted attackers to execute arbitrary code via a crafted archive (such as ZIP) that contains long path names, which triggers an error in the BOMStackPop function.

CVE-2006-1985 has been assigned by [M cve@mitre.org](mailto:cve@mitre.org) to track the vulnerability

CVSS2 Score: 5.1 - MEDIUM

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

CVE References

Description	Tags	Link
Apple Mac OS X Security Update 2006-003 Multiple Vulnerabilities	cve.report (archive) text/html	🌐 BID 17951
Webmail : Solution de messagerie professionnelle - OVHcloud-OVH	Vendor Advisory www.vupen.com text/html	🌐 VUPEN ADV-2006-1779
Webmail - OVH	Vendor Advisory www.vupen.com text/html	🌐 VUPEN ADV-2006-1452
APPLE-SA-2006-05-11 Security Update 2006-003	Patch lists.apple.com text/html	🍏 APPLE APPLE-SA-2006-05-11

Security-Protocols :: Computer Security Research	Patch Vendor Advisory web.archive.org text/html Inactive Link Not Archived	MISC www.security-protocols.com/sp-x25-advisory.php
Mac OS X Security Update Fixes Multiple Vulnerabilities - Advisories - Secunia	Patch Vendor Advisory web.archive.org text/html	X SECUNIA 20077
No Description Provided	www.security-protocols.com text/html Inactive Link Not Archived	MISC www.security-protocols.com/modules.php?name=News&file=article&sid=3233
US-CERT Technical Cyber Security Alert TA06-132A -- Apple Mac Products Affected by Multiple Vulnerabilities	Patch Third Party Advisory US Government Resource www.us-cert.gov text/html	F CERT TA06-132A
No Description Provided	www.osvdb.org Inactive Link Not Archived	G OSVDB 24819
IBM X-Force Exchange	exchange.xforce.ibmcloud.com text/html	F XF macosx-archivehelper-bo(25945)
Apple Mac OS X Multiple Security Vulnerabilities	cve.report (archive) text/html	G BID 17634
SecurityTracker.com Archives - Apple Mac OS X Kernel Components Let Remote Users Execute Arbitrary Code	securitytracker.com text/html	G SECTrack 1016082
Mac OS X Multiple Potential Vulnerabilities - Advisories - Secunia	Vendor Advisory web.archive.org text/html	X SECUNIA 19686

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	Mac Os X	10.3	All	All	All
Operating System	Apple	Mac Os X	10.3.1	All	All	All
Operating System	Apple	Mac Os X	10.3.2	All	All	All
Operating System	Apple	Mac Os X	10.3.3	All	All	All
Operating System	Apple	Mac Os X	10.3.4	All	All	All
Operating System	Apple	Mac Os X	10.3.5	All	All	All

Operating System	Apple	Mac Os X	10.3.5	All	All	All
Operating System	Apple	Mac Os X	10.3.6	All	All	All
Operating System	Apple	Mac Os X	10.3.7	All	All	All
Operating System	Apple	Mac Os X	10.3.8	All	All	All
Operating System	Apple	Mac Os X	10.3.9	All	All	All
Operating System	Apple	Mac Os X	10.4	All	All	All
Operating System	Apple	Mac Os X	10.4.1	All	All	All
Operating System	Apple	Mac Os X	10.4.2	All	All	All
Operating System	Apple	Mac Os X	10.4.3	All	All	All
Operating System	Apple	Mac Os X	10.4.4	All	All	All
Operating System	Apple	Mac Os X	10.4.5	All	All	All
Operating System	Apple	Mac Os X	10.4.6	All	All	All
Operating System	Apple	Mac Os X	10.3	All	All	All
Operating System	Apple	Mac Os X	10.3.1	All	All	All
Operating System	Apple	Mac Os X	10.3.2	All	All	All
Operating System	Apple	Mac Os X	10.3.3	All	All	All
Operating System	Apple	Mac Os X	10.3.4	All	All	All
Operating System	Apple	Mac Os X	10.3.5	All	All	All
Operating System	Apple	Mac Os X	10.3.6	All	All	All
Operating System	Apple	Mac Os X	10.3.7	All	All	All
Operating System	Apple	Mac Os X	10.3.8	All	All	All
Operating System	Apple	Mac Os X	10.3.9	All	All	All
Operating System	Apple	Mac Os X	10.4	All	All	All

Operating System	Apple	Mac Os X	10.4.1	All	All	All
Operating System	Apple	Mac Os X	10.4.2	All	All	All
Operating System	Apple	Mac Os X	10.4.3	All	All	All
Operating System	Apple	Mac Os X	10.4.4	All	All	All
Operating System	Apple	Mac Os X	10.4.5	All	All	All
Operating System	Apple	Mac Os X	10.4.6	All	All	All
Operating System	Apple	Mac Os X Server	10.3	All	All	All
Operating System	Apple	Mac Os X Server	10.3.1	All	All	All
Operating System	Apple	Mac Os X Server	10.3.2	All	All	All
Operating System	Apple	Mac Os X Server	10.3.3	All	All	All
Operating System	Apple	Mac Os X Server	10.3.4	All	All	All
Operating System	Apple	Mac Os X Server	10.3.5	All	All	All
Operating System	Apple	Mac Os X Server	10.3.6	All	All	All
Operating System	Apple	Mac Os X Server	10.3.7	All	All	All
Operating System	Apple	Mac Os X Server	10.3.8	All	All	All
Operating System	Apple	Mac Os X Server	10.3.9	All	All	All
Operating System	Apple	Mac Os X Server	10.4	All	All	All
Operating System	Apple	Mac Os X Server	10.4.1	All	All	All
Operating System	Apple	Mac Os X Server	10.4.2	All	All	All
Operating System	Apple	Mac Os X Server	10.4.3	All	All	All
Operating System	Apple	Mac Os X Server	10.4.4	All	All	All
Operating System	Apple	Mac Os X Server	10.4.5	All	All	All
Operating System	Apple	Mac Os X Server	10.4.6	All	All	All

cpe:2.3:o:apple:mac_os_x:10.3.1:*****:
cpe:2.3:o:apple:mac_os_x:10.3.2:*****:
cpe:2.3:o:apple:mac_os_x:10.3.3:*****:
cpe:2.3:o:apple:mac_os_x:10.3.4:*****:
cpe:2.3:o:apple:mac_os_x:10.3.5:*****:
cpe:2.3:o:apple:mac_os_x:10.3.6:*****:
cpe:2.3:o:apple:mac_os_x:10.3.7:*****:
cpe:2.3:o:apple:mac_os_x:10.3.8:*****:
cpe:2.3:o:apple:mac_os_x:10.3.9:*****:
cpe:2.3:o:apple:mac_os_x:10.4:*****:
cpe:2.3:o:apple:mac_os_x:10.4.1:*****:
cpe:2.3:o:apple:mac_os_x:10.4.2:*****:
cpe:2.3:o:apple:mac_os_x:10.4.3:*****:
cpe:2.3:o:apple:mac_os_x:10.4.4:*****:
cpe:2.3:o:apple:mac_os_x:10.4.5:*****:
cpe:2.3:o:apple:mac_os_x:10.4.6:*****:
cpe:2.3:o:apple:mac_os_x:10.3:*****:
cpe:2.3:o:apple:mac_os_x:10.3.1:*****:
cpe:2.3:o:apple:mac_os_x:10.3.2:*****:
cpe:2.3:o:apple:mac_os_x:10.3.3:*****:
cpe:2.3:o:apple:mac_os_x:10.3.4:*****:
cpe:2.3:o:apple:mac_os_x:10.3.5:*****:
cpe:2.3:o:apple:mac_os_x:10.3.6:*****:
cpe:2.3:o:apple:mac_os_x:10.3.7:*****:
cpe:2.3:o:apple:mac_os_x:10.3.8:*****:
cpe:2.3:o:apple:mac_os_x:10.3.9:*****:
cpe:2.3:o:apple:mac_os_x:10.4:*****:
cpe:2.3:o:apple:mac_os_x:10.4.1:*****:
cpe:2.3:o:apple:mac_os_x:10.4.2:*****:

cpe:2.3:o:apple:mac_os_x:10.4.2:*:*:*:*:*:
cpe:2.3:o:apple:mac_os_x:10.4.3:*:*:*:*:*:
cpe:2.3:o:apple:mac_os_x:10.4.4:*:*:*:*:*:
cpe:2.3:o:apple:mac_os_x:10.4.5:*:*:*:*:*:
cpe:2.3:o:apple:mac_os_x:10.4.6:*:*:*:*:*:
cpe:2.3:o:apple:mac_os_x_server:10.3:*:*:*:*:*:
cpe:2.3:o:apple:mac_os_x_server:10.3.1:*:*:*:*:*:
cpe:2.3:o:apple:mac_os_x_server:10.3.2:*:*:*:*:*:
cpe:2.3:o:apple:mac_os_x_server:10.3.3:*:*:*:*:*:
cpe:2.3:o:apple:mac_os_x_server:10.3.4:*:*:*:*:*:
cpe:2.3:o:apple:mac_os_x_server:10.3.5:*:*:*:*:*:
cpe:2.3:o:apple:mac_os_x_server:10.3.6:*:*:*:*:*:
cpe:2.3:o:apple:mac_os_x_server:10.3.7:*:*:*:*:*:
cpe:2.3:o:apple:mac_os_x_server:10.3.8:*:*:*:*:*:
cpe:2.3:o:apple:mac_os_x_server:10.3.9:*:*:*:*:*:
cpe:2.3:o:apple:mac_os_x_server:10.4:*:*:*:*:*:
cpe:2.3:o:apple:mac_os_x_server:10.4.1:*:*:*:*:*:
cpe:2.3:o:apple:mac_os_x_server:10.4.2:*:*:*:*:*:
cpe:2.3:o:apple:mac_os_x_server:10.4.3:*:*:*:*:*:
cpe:2.3:o:apple:mac_os_x_server:10.4.4:*:*:*:*:*:
cpe:2.3:o:apple:mac_os_x_server:10.4.5:*:*:*:*:*:
cpe:2.3:o:apple:mac_os_x_server:10.4.6:*:*:*:*:*:
cpe:2.3:o:apple:mac_os_x_server:10.3:*:*:*:*:*:
cpe:2.3:o:apple:mac_os_x_server:10.3.1:*:*:*:*:*:
cpe:2.3:o:apple:mac_os_x_server:10.3.2:*:*:*:*:*:
cpe:2.3:o:apple:mac_os_x_server:10.3.3:*:*:*:*:*:
cpe:2.3:o:apple:mac_os_x_server:10.3.4:*:*:*:*:*:
cpe:2.3:o:apple:mac_os_x_server:10.3.5:*:*:*:*:*:
cpe:2.3:o:apple:mac_os_x_server:10.3.6:*:*:*:*:*:

cpe:2.3:o:apple:mac_os_x_server:10.3.7:*****:
cpe:2.3:o:apple:mac_os_x_server:10.3.8:*****:
cpe:2.3:o:apple:mac_os_x_server:10.3.9:*****:
cpe:2.3:o:apple:mac_os_x_server:10.4:*****:
cpe:2.3:o:apple:mac_os_x_server:10.4.1:*****:
cpe:2.3:o:apple:mac_os_x_server:10.4.2:*****:
cpe:2.3:o:apple:mac_os_x_server:10.4.3:*****:
cpe:2.3:o:apple:mac_os_x_server:10.4.4:*****:
cpe:2.3:o:apple:mac_os_x_server:10.4.5:*****:
cpe:2.3:o:apple:mac_os_x_server:10.4.6:*****:
cpe:2.3:a:apple:safari:2.0:*****:
cpe:2.3:a:apple:safari:2.0.1:*****:
cpe:2.3:a:apple:safari:2.0.2:*****:
cpe:2.3:a:apple:safari:2.0.3:*****:
cpe:2.3:a:apple:safari:2.0:*****:
cpe:2.3:a:apple:safari:2.0.1:*****:
cpe:2.3:a:apple:safari:2.0.2:*****:
cpe:2.3:a:apple:safari:2.0.3:*****:

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](#)