



CVE-2007-0724

[MITRE](#)[NVD](#)[CVE.ORG](#)[JSON API](#)[Print: PDF](#)

Summary

CVE	CVE-2007-0724
State	PUBLISHED
Assigner	mitre
Source Priority	CVE Program / NVD first with legacy fallback
Published	2007-03-13 22:19:00 UTC
Updated	2026-04-23 00:35:47 UTC
Description	The IOKit HID interface in Apple Mac OS X 10.3.9 and 10.4 through 10.4.8 does not sufficiently limit access to certain contr

Risk And Classification

Primary CVSS: v2.0 6.9 from nvd@nist.gov

AV:L/AC:M/Au:N/C:C/I:C/A:C

Problem Types: NVD-CWE-Other | n/a

CVSS v2.0 Breakdown

Access Vector

Local

Access Complexity

Medium

Authentication

None

Confidentiality

Complete

Integrity

Complete

Availability

Complete

AV:L/AC:M/Au:N/C:C/I:C/A:C

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
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	10.4.7	All	All	All
Operating System	Apple	Mac Os X	10.4.8	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
Operating System	Apple	Mac Os X Server	10.4.7	All	All	All
Operating System	Apple	Mac Os X Server	10.4.8	All	All	All

Vendor Declared Affected Products						
Source	Vendor	Product	Version	Platforms		
CNA	Na	N/a	affected n/a	Not specified		

References
Reference
About Security Update 2007-004
APPLE-SA-2007-03-13 Mac OS X v10.4.9 and Security Update 2007-003
Webmail - OVH
www.osvdb.org/34855
US-CERT Technical Cyber Security Alert TA07-072A -- Apple Updates for Multiple Vulnerabilities
SecurityTracker.com Archives - Mac OS X Lets Remote Users Execute Arbitrary Code and Local Users Obtain Elevated Privileges and Deny S
APPLE-SA-2007-04-19 Security Update 2007-004
Mac OS X Security Update Fixes Multiple Vulnerabilities - Advisories - Secunia
About the security content of Mac OS X 10.4.9 and Security Update 2007-003
SecurityTracker.com Archives - Mac OS X Bugs Let Remote Users Execute Arbitrary Code and Local Users Gain Elevated Privileges
Webmail - OVH
IBM X Force Exchange

IBM X-Force Exchange
US-CERT Technical Cyber Security Alert TA07-109A -- Apple Updates for Multiple Vulnerabilities
Apple Mac OS X Multiple Applications Multiple Vulnerabilities
Mac OS X Security Update Fixes Multiple Vulnerabilities - Advisories - Secunia
CVE Program record
NVD vulnerability detail

No vendor comments have been submitted for this CVE.
There are currently no legacy QID mappings associated with this CVE.

© [CVE.report](#) 2026 |

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](#).

Free CVE JSON API [cve.report/api](#)

CVE.report and Source URL Uptime Status [status.cve.report](#)