



CVE-2007-0726

- MITRE
- NVD
- CVE.ORG
- JSON API
- Print: PDF

Summary

CVE	CVE-2007-0726
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 SSH key generation process in OpenSSH in Apple Mac OS X 10.3.9 and 10.4 through 10.4.8 allows remote attackers to

Risk And Classification

Primary CVSS: v2.0 5 from nvd@nist.gov

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

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

CVSS v2.0 Breakdown

Access Vector

Network

Access Complexity

Low

Authentication

None

Confidentiality

None

Integrity

None

Availability

Partial

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

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	10.3.9	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
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	Source
APPLE-SA-2007-03-13 Mac OS X v10.4.9 and Security Update 2007-003	af854a3a-2127-422b-91ae-364da266110d
Webmail - OVH	af854a3a-2127-422b-91ae-364da266110d
US-CERT Technical Cyber Security Alert TA07-072A -- Apple Updates for Multiple Vulnerabilities	af854a3a-2127-422b-91ae-364da266110d
Mac OS X Security Update Fixes Multiple Vulnerabilities - Advisories - Secunia	af854a3a-2127-422b-91ae-364da266110d
About the security content of Mac OS X 10.4.9 and Security Update 2007-003	af854a3a-2127-422b-91ae-364da266110d
Apple OpenSSH Key Generation Process Lets Remote Users Deny Service - SecurityTracker	af854a3a-2127-422b-91ae-364da266110d
www.osvdb.org/34850	af854a3a-2127-422b-91ae-364da266110d
IBM X-Force Exchange	af854a3a-2127-422b-91ae-364da266110d
Apple Mac OS X Multiple Applications Multiple Vulnerabilities	af854a3a-2127-422b-91ae-364da266110d
CVE Program record	CVE.ORG
NVD vulnerability detail	NVD

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](#)