



CVE-2014-1266

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

Summary

CVE	CVE-2014-1266
State	PUBLISHED
Assigner	apple
Source Priority	CVE Program / NVD first with legacy fallback
Published	2014-02-22 17:05:21 UTC
Updated	2026-04-29 01:13:23 UTC
Description	The SSLVerifySignedServerKeyExchange function in libsecurity_ssl/lib/sslKeyExchange.c in the Secure Transport feature i

Risk And Classification

Primary CVSS: v3.1 7.4 HIGH from nvd@nist.gov

CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:N

Problem Types: CWE-295 | n/a

Version	Source	Type	Score	Severity	Vector
3.1	nvd@nist.gov	Primary	7.4	HIGH	CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:N
2.0	nvd@nist.gov	Primary	5.8		AV:N/AC:M/Au:N/C:P/I:P/A:N

CVSS v3.1 Breakdown

Attack Vector

Network

Attack Complexity

High

Privileges Required

None

User Interaction

None

Scope

Unchanged

Confidentiality

High

Integrity

High

Availability

None

CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:N

CVSS v2.0 Breakdown

Access Vector

Network

Access Complexity

Medium

Authentication

None

Confidentiality

Partial

Integrity

Partial

Availability

None

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

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Apple	Iphone Os	All	All	All	All

Vendor Declared Affected Products

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

References

Reference	Source
About the security content of iOS 6.1.6	af854a3a-2127-422b-91ae-364da266
SMBlog -- 24 February 2014	af854a3a-2127-422b-91ae-364da266
About the security content of OS X Mavericks v10.9.2 and Security Update 2014-001 - Apple Support	af854a3a-2127-422b-91ae-364da266
SMBlog -- 23 February 2014	af854a3a-2127-422b-91ae-364da266
About the security content of Apple TV 6.0.2 - Apple Support	af854a3a-2127-422b-91ae-364da266
About the security content of iOS 7.0.6 - Apple Support	af854a3a-2127-422b-91ae-364da266
ImperialViolet - Apple's SSL/TLS bug	af854a3a-2127-422b-91ae-364da266
Apple Fixes Dangerous SSL Authentication Flaw In iOS - Slashdot	af854a3a-2127-422b-91ae-364da266
Take a look at http://opensource.apple.com/source/Security/Security-55471/libsec... Hacker News	af854a3a-2127-422b-91ae-364da266
CVE Program record	CVE.ORG

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](#)