



CVE-2008-4368

Published on: 10/01/2008 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:25:10 PM UTC

CVE-2008-4368

[Source: Mitre](#)

[Source: NIST](#)

[CVE.ORG](#)

[Print: PDF](#)



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

The default configuration of Java 1.5 on Apple Mac OS X 10.5.4 and 10.5.5 contains a jurisdiction policy that limits Java Cryptography Extension (JCE) key sizes to 128 bits, which makes it easier for attackers to decrypt ciphertext produced by JCE.

CVE-2008-4368 has been assigned by [M](#) cve@mitre.org to track the vulnerability

CVSS2 Score: **5 - MEDIUM**

Access
Vector

NETWORK

Access
Complexity

LOW

Authentication

NONE

Confidentiality
Impact

PARTIAL

Integrity
Impact

NONE

Availability
Impact

NONE

CVE References

Description

Tags

Link

IBM X-Force Exchange

[exchange.xforce.ibmcloud.com](https://exchange.xforce.ibmcloud.com/text/html)
[text/html](#)

[XF java-jce-information-disclosure\(45650\)](#)

About the security content of Java for Mac OS X 10.5 Update 2

[support.apple.com](https://support.apple.com/text/html)
[text/html](#)

[CONFIRM](#)
support.apple.com/kb/HT3179

APPLE-SA-2008-09-24 Java for Mac OS X 10.5 Update 2

[lists.apple.com](https://lists.apple.com/text/html)
[text/html](#)

[APPLE APPLE-SA-2008-09-24](#)

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	10.5.4	All	All	All
Operating System	Apple	Mac Os X	10.5.5	All	All	All
Operating System	Apple	Mac Os X	10.5.4	All	All	All
Operating System	Apple	Mac Os X	10.5.5	All	All	All
cpe:2.3:o:apple:mac_os_x:10.5.4:*:*:*:*:*:						
cpe:2.3:o:apple:mac_os_x:10.5.5:*:*:*:*:*:						
cpe:2.3:o:apple:mac_os_x:10.5.4:*:*:*:*:*:						
cpe:2.3:o:apple:mac_os_x:10.5.5:*:*:*:*:*:						

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](#)