



CVE-2008-0994

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

Summary

CVE	CVE-2008-0994
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2008-03-18 23:44:00 UTC
Updated	2017-08-08 01:29:00 UTC
Description	Preview in Apple Mac OS X 10.5.2 uses 40-bit RC4 when saving a PDF file with encryption, which makes it easier for attack

Risk And Classification

Problem Types: CWE-200

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Apple	Mac Os X	10.5.2	All	All	All
Operating System	Apple	Mac Os X	10.5.2	All	All	All
Operating System	Apple	Mac Os X Server	10.5.2	All	All	All
Operating System	Apple	Mac Os X Server	10.5.2	All	All	All

References

Reference	Source	Link
About Security Update 2008-002	CONFIRM	docs.apple.com
US-CERT Technical Cyber Security Alert TA08-079A -- Apple Updates for Multiple Vulnerabilities	CERT	www.us-cert.gov
IBM X-Force Exchange	XF	exchange.xforce.ibmcloud.com
Mac OS X Security Update Fixes Multiple Vulnerabilities - Secunia Advisories - Vulnerability Intelligence - Secunia.com	SECUNIA	secunia.com
Webmail : Solution de messagerie professionnelle - OVHcloud- OVH	VUPEN	www.ovh.com
SecurityTracker.com Archives - Mac OS X Preview Saves Encrypted PDF Files Using Weak Encryption	SECTrack	www.securitytracker.com
Apple Mac OS X Preview PDF Insecure Encryption Weakness	BID	www.bids.cisco.com
RETIRED: Apple Mac OS X 2008-002 Multiple Security Vulnerabilities	BID	www.bids.cisco.com
APPLE-SA-2008-03-18 Security Update 2008-002	APPLE	lists.apple.com
CVE Program record	CVE.ORG	www.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](#)