



CVE-2003-0420

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

Summary

CVE	CVE-2003-0420
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2003-06-13 04:00:00 UTC
Updated	2017-07-11 01:29:00 UTC
Description	Information leak in dsimportexport for Apple Macintosh OS X Server 10.2.6 allows local users to obtain the username and p

Risk And Classification

Problem Types: NVD-CWE-Other

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Apple	Mac Os X Server	10.2.6	All	All	All
Operating System	Apple	Mac Os X Server	10.2.6	All	All	All

References

Reference
Secunia - Advisories - Mac OS X Security Update for Apache and dsimportexport
Apple Mac OS X DSIMPORTEXPOR Information Disclosure Weakness
AusCERT - ESB-2003.0415 -- APPLE-SA-2003-06-12 Security Update 2003-06-12 -- Security holes in the Apache 2.0.x mod_dav module and
Apple Computer Inc. Information for VU#757612
IBM X-Force Exchange
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](#)