



CVE-2005-4217

Published on: 12/14/2005 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:27:21 PM UTC

CVE-2005-4217

Source: Mitre

Source: NIST

CVE.ORG

Print: PDF



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

Perl in Apple Mac OS X Server 10.3.9 does not properly drop privileges when using the "\$<" variable to set uid, which allows attackers to gain privileges.

CVE-2005-4217 has been assigned by [M](#) cve@mitre.org to track the vulnerability

CVSS2 Score: **7.5 - HIGH**

Access
Vector

Access
Complexity

Authentication

NETWORK

LOW

NONE

Confidentiality
Impact

Integrity
Impact

Availability
Impact

PARTIAL

PARTIAL

PARTIAL

CVE References

Description

Tags

Link

Mac OS X Security Update Fixes Multiple Vulnerabilities - Advisories - Secunia

[Vendor Advisory](#)
[web.archive.org](#)
[text/html](#)

[X](#) [SECUNIA 19064](#)

Webmail : Solution de messagerie professionnelle - OVHcloud- OVH

[Vendor Advisory](#)
[www.vupen.com](#)
[text/html](#)

[VUPEN ADV-2006-0791](#)

Secunia - Advisories - Mac OS X Perl "\$<" Privilege Dropping Security Issue

[Vendor Advisory](#)
[web.archive.org](#)
[text/html](#)

[X](#) [SECUNIA 17922](#)

Apple Mac OS X Perl Insecure Privilege Dropping Weakness

[cve.report \(archive\)](#)
[text/html](#)

[BID 15833](#)

IBM X-Force Exchange

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

[XF macos-perl-bypass-security\(23561\)](#)

APPLE-SA-2006-03-01 Security Update 2006-001	lists.apple.com text/html	 APPLE APPLE-SA-2006-03-01
Apple Mac OS X Security Update 2006-001 Multiple Vulnerabilities	cve.report (archive) text/html	 BID 16907
Webmail : Solution de messagerie professionnelle - OVHcloud- OVH	Vendor Advisory www.vupen.com text/html	 VUPEN ADV-2005-2869
About Security Update 2006-001	web.archive.org text/html Inactive Link Not Archived	 CONFIRM docs.info.apple.com/article.html?artnum=303382
US-CERT Technical Cyber Security Alert TA06-062A -- Apple Mac Products are Affected by Multiple Vulnerabilities	US Government Resource www.us-cert.gov text/html	 CERT TA06-062A
No Description Provided	www.osvdb.org Inactive Link Not Archived	 OSVDB 21800

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 Server	10.3.9	All	All	All
Operating System	Apple	Mac Os X Server	10.3.9	All	All	All
cpe:2.3:o:apple:mac_os_x_server:10.3.9:****:***:						
cpe:2.3:o:apple:mac_os_x_server:10.3.9:****:***:						

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](#)