

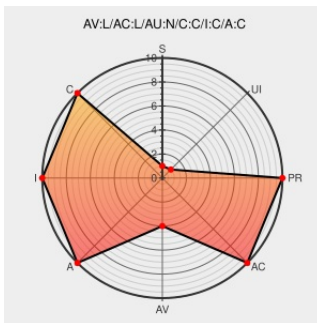


CVE-2003-0703

Published on: 09/12/2003 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:28:44 PM UTC

CVE-2003-0703

[Source: Mitre](#)[Source: NIST](#)[CVE.ORG](#)[Print: PDF](#) 

Certain versions of [Kismac](#) from [Kismac](#) contain the following vulnerability:

KisMAC before 0.05d trusts user-supplied variables to load arbitrary kernels or kernel modules, which allows local users to gain privileges via the \$DRIVER_KEXT environment variable as used in (1) viha_driver.sh, (2) macjack_load.sh, or (3) airojack_load.sh, or (4) via "similar techniques" using exchangeKernel.sh.

CVE-2003-0703 has been assigned by [M](#) cve@mitre.org to track the vulnerability

CVSS2 Score: **7.2 - HIGH**

Access
Vector

LOCAL

Access
Complexity

LOW

Authentication

NONE

Confidentiality
Impact

COMPLETE

Integrity
Impact

COMPLETE

Availability
Impact

COMPLETE

CVE References

Description

Tags

Link

IBM X-Force Exchange

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

[XF kismac-driverkext-load-modules\(13007\)](#)

[Patch](#)
[Vendor Advisory](#)
[www.atstake.com](#)
[text/plain](#)
[Inactive Link](#) [Not Archived](#)

[ATSTAKE A082203-1](#)

IBM X-Force Exchange

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

[XF kismac-exchangekernel-kernel-overwrite\(13008\)](#)

KisMAC Multiple Local Privilege Escalation
Vulnerabilities

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

[BID 8497](#)

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
Application	Kismac	Kismac	0.05d	All	All	All
Application	Kismac	Kismac	0.05d	All	All	All
cpe:2.3:a:kismac:kismac:0.05d:~::~::~:						
cpe:2.3:a:kismac:kismac:0.05d:~::~::~:						

No vendor comments have been submitted for this CVE

[← Previous ID](#)

[Next ID →](#)