



CVE-2008-2926

[MITRE](#)[NVD](#)[CVE.ORG](#)[Print: PDF !\[\]\(e3f8612927870f2e0f9f5989e6dd3064_img.jpg\)](#)

Summary

CVE	CVE-2008-2926
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2008-08-12 23:41:00 UTC
Updated	2021-04-09 17:08:00 UTC
Description	The kmxfw.sys driver in CA Host-Based Intrusion Prevention System (HIPS) r8, as used in CA Internet Security Suite and F

Risk And Classification

Problem Types: CWE-20

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Broadcom	Internet Security Suite	3.0	All	All	All
Application	Ca	Host Based Intrusion Prevention System	r8	All	All	All
Application	Ca	Host Based Intrusion Prevention System	r8	All	All	All
Application	Ca	Internet Security Suite	3.0	All	All	All
Application	Ca	Internet Security Suite	3.0	All	All	All
Application	Ca	Internet Security Suite 2008	All	All	All	All
Application	Ca	Internet Security Suite 2008	All	All	All	All
Application	Ca	Personal Firewall 2007	All	All	All	All
Application	Ca	Personal Firewall 2007	All	All	All	All
Application	Ca	Personal Firewall 2008	All	All	All	All
Application	Ca	Personal Firewall 2008	All	All	All	All

References

Reference

Computer Associates 'kmxfw.sys' Local Code Execution and Remote Denial of Service Vulnerabilities

CA Personal Firewall 'kmxfw.sys' IOCTL Validation Flaw Lets Local Users Gain Elevated Privileges - SecurityTracker

CA Products kmxfw.sys Privilege Escalation and Denial of Service - Secunia.com

CA Internet Security 'kmxfw.sys' IOCTL Validation Flaw Lets Local Users Gain Elevated Privileges - SecurityTracker

Webmail : Solution de messagerie professionnelle - OVHcloud- OVH

SecurityFocus

CA Host-Based Intrusion Prevention System 'kmxfw.sys' IOCTL Validation Flaw Lets Local Users Gain Elevated Privileges - SecurityTracker

CA HIPS kmxfw.sys IOCTL requests arbitrary code execution vulnerability - CA

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](#).

CVE.report and Source URL Uptime Status [status.cve.report](#)