



CVE-2006-3999

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

Summary

CVE	CVE-2006-3999
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2006-08-05 01:04:00 UTC
Updated	2018-10-17 21:32:00 UTC
Description	ISS BlackICE PC Protection 3.6.cpj, 3.6.cpiE, and possibly earlier versions do not properly monitor the integrity of the pamv

Risk And Classification

Problem Types: NVD-CWE-Other

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Iss	Blackice Pc Protection	3.6cpie	All	All	All
Application	Iss	Blackice Pc Protection	3.6cpj	All	All	All
Application	Iss	Blackice Pc Protection	3.6cpie	All	All	All
Application	Iss	Blackice Pc Protection	3.6cpj	All	All	All

References

Reference	Source
SecurityTracker.com Archives - BlackICE Insufficient Access Controls on 'pamversion.dll' Lets Local Users Gain Elevated Privileges	SECTF
SecurityFocus	BUGTF
SecurityReason - ISS BlackICE PC Protection DLL faking of run-time linked libraries Vulnerability	SREAS
CVE Program record	CVE.O
NVD vulnerability detail	NVD

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](#)