



CVE-2005-2711

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

Summary

CVE	CVE-2005-2711
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2005-12-31 05:00:00 UTC
Updated	2017-07-11 01:32:00 UTC
Description	ISS Blacklce 3.6, as used in multiple products including BlackICE PC Protection, Server Protection, Agent for Server, and F

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 Agent Server	All	All	All	All
Application	Iss	Blackice Agent Server	All	All	All	All
Application	Iss	Blackice Pc Protection	3.6	All	All	All
Application	Iss	Blackice Pc Protection	3.6cpu	All	All	All
Application	Iss	Blackice Pc Protection	3.6	All	All	All
Application	Iss	Blackice Pc Protection	3.6cpu	All	All	All
Application	Iss	Blackice Server Protection	All	All	All	All
Application	Iss	Blackice Server Protection	All	All	All	All
Application	Iss	Realsecure Desktop	3.6	All	All	All
Application	Iss	Realsecure Desktop	7.0	All	All	All
Application	Iss	Realsecure Desktop	3.6	All	All	All
Application	Iss	Realsecure Desktop	7.0	All	All	All

References

Reference	Source	Link
Accenture Let there be change	IDEFENSE	www.idefense.com
IBM X-Force Exchange	XF	exchange.xforce.ibmclm.com

Webmail : Solution de messagerie professionnelle - OVHcloud- OVH	VUPEN	www.vupen.com
BlackICE Help System Lets Local Users Gain Elevated Privileges - SecurityTracker	SECTRACK	securitytracker.com
24096	OSVDB	www.osvdb.org
RealSecure Desktop Help System Lets Local Users Gain Elevated Privileges - SecurityTracker	SECTRACK	securitytracker.com
Internet Security Systems BlackICE and RealSecure Desktop Local Privilege Escalation Vulnerability	BID	www.securityfocus.com
Secunia - Advisories - ISS Products Application Protection Module Privilege Escalation	SECUNIA	secunia.com
CVE Program record	CVE.ORG	www.cve.org
NVD vulnerability detail	NVD	nvd.nist.gov

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