

# [NT] ISS Multiple Products Local Privilege Escalation

---

*Source:* <http://www.derkeiler.com/Mailing-Lists/Securiteam/2006-03/msg00079.html>

---

- *From:* SecuriTeam <[support@xxxxxxxxxxxxxxx](mailto:support@xxxxxxxxxxxxxxx)>
  - *Date:* 26 Mar 2006 15:58:02 +0200
- 

The following security advisory is sent to the securiteam mailing list, and can be found at the SecuriTeam web site: <http://www.securiteam.com>  
-- promotion

The SecuriTeam alerts list – Free, Accurate, Independent.

Get your security news from a reliable source.  
<http://www.securiteam.com/maillinglist.html>

-----

## ISS Multiple Products Local Privilege Escalation

---

### SUMMARY

<[http://www.iss.net/products\\_services/products.php](http://www.iss.net/products_services/products.php)> Internet Security Systems (ISS) has developed a suite of tools aimed at securing server and desktop systems. A flaw exists within a central module to these components that can allow unprivileged users to obtain complete control of the machine.

Local exploitation of a design error in the multiple Internet Security Systems (ISS) products may allow a user to gain System level privileges. Exploitation of this issue is trivial and can be done manually.

### DETAILS

Vulnerable Systems:

- \* Vulnerability found exists in version 3.6 of ISS BlackIce PC Desktop for Windows with all current updates applied.

This exploit has been confirmed in ISS BlackIce 3.6 product and is reportedly also found in the following products:

- BlackICE PC Protection (Consumer)

## [NT] ISS Multiple Products Local Privilege Escalation

- BlackICE Server Protection (Consumer)
- BlackICE Agent for Server (Corporate)
- RealSecure Desktop 3.6 and 7.0 (Corporate)

To exploit this condition you must first trigger an action that would initiate the Application Protection Module to display a warning. For the BlackIce product, this can be initiated by launching any executable moved or installed after the product itself was first installed.

From the "Application Protection" dialog press the "More Info" button with will bring up a secondary form. With this form active, pressing the F1 key will bring up the standard Windows Open File dialog prompting the user to manually locate the help file for the application.

The problem arises when the BlackIce process fails to drop permissions before launching the help dialog. If a user resets the dialog file mask by entering \*.exe [enter] they can then launch any executable on the system from the dialog by right clicking on it and choosing "open". Applications run in this manner will be executed with System level rights.

Successful exploitation allows a local attacker to execute arbitrary commands as the System Administrator user. This allows complete system compromise including the installation and removal of applications, and ability to read and write any file on the system.

### CVE Information:

<<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2005-2711>>  
CAN-2005-2711

### Disclosure Timeline:

- \* 23.08.05 – Initial vendor notification
- \* 24.08.05 – Initial vendor response
- \* 23.03.06 – Public disclosure

### ADDITIONAL INFORMATION

The information has been provided by iDefense.

The original article can be found at:

<<http://www.ndefense.com/intelligence/vulnerabilities/display.php?id=403>>  
<http://www.ndefense.com/intelligence/vulnerabilities/display.php?id=403>

=====

This bulletin is sent to members of the SecuriTeam mailing list.

To unsubscribe from the list, send mail with an empty subject line and body to:

[NT] ISS Multiple Products Local Privilege Escalation

list-unsubscribe@xxxxxxxxxxxxxxxxx

In order to subscribe to the mailing list, simply forward this email to: list-subscribe@xxxxxxxxxxxxxxxxx

=====  
=====

**DISCLAIMER:**

The information in this bulletin is provided "AS IS" without warranty of any kind.

In no event shall we be liable for any damages whatsoever including direct, indirect, incidental, consequential, loss of business profits or special damages.