

[NT] BlackICE Agent not Firewalling after Standby

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2002-06/0024.html>

From: support@securiteam.com

Date: 06/08/02

From: support@securiteam.com

To: list@securiteam.com

Date: Sat, 8 Jun 2002 22:50:37 +0200 (CEST)

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

When was the last time you checked your server's security?

How about a monthly report?

<http://www.AutomatedScanning.com> -- Know that you're safe.

BlackICE Agent not Firewalling after Standby

SUMMARY

In a default installation, The BlackICE Agent might not reactivate when the host returns from standby. This could allow a malicious user to bypass the firewall completely.

DETAILS

Vulnerable systems:

- * BlackICE Agent 3.1 eal on Windows 2000 laptop

Immune systems:

- * BlackICE Agent 3.1 ebh on Windows 2000 laptop

The BlackICE Agent setup contains the parameter "restart.whenSuspend", which should be enabled by default. This, however, is not always the case, and as a result, the firewall might not reactivate after a system standby.

The BlackICE Agent would still give all the appearances of being active, but the filter function would not be in effect, and network communication would be possible to the same extent as if the software was not installed.

Vendor response:

The vendor was notified on 15 March 2002. The issue was assigned case number 526997. On 18 March, we received a workaround that seemingly solved

Securiteam: [NT] BlackICE Agent not Firewalling after Standby

the issue. On 6 June 2002, the vendor informed us that the issue had been corrected in the latest build.

Corrective action:

Upgrade to BlackICE Agent V3.1 EBH, available through:

<<https://bvlive01.iss.net/issEn/DLC/login.jhtml>>

<https://bvlive01.iss.net/issEn/DLC/login.jhtml>

ADDITIONAL INFORMATION

The information has been provided by <mailto:asandor@kpmg.dk> Andreas Sandor.

=====

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:

list-unsubscribe@securiteam.com

In order to subscribe to the mailing list, simply forward this email to: list-subscribe@securiteam.com

=====

=====

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.

-
- *Previous message:* support@securiteam.com: "[\[NEWS\] Multiple Vulnerabilities in Novell Netware](#)"
 - *Messages sorted by:* [\[date \]](#) [\[thread \]](#) [\[subject \]](#) [\[author \]](#) [\[attachment \]](#)