

[NT] Denial of Service in Sabre Desktop Reservation Client for Windows

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2002-10/0063.html>

From: support@securiteam.com

Date: 10/16/02

From: support@securiteam.com

To: list@securiteam.com

Date: 16 Oct 2002 23:56:02 +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

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.

Denial of Service in Sabre Desktop Reservation Client for Windows

SUMMARY

Sabre Desktop Reservation Software for Windows has a component called Sabserv (listening on TCP port 1001) that connects the client application to the communication components and eventually to the local Sabre gateway at the local site. If Sabserv is sent arbitrary data on TCP port 1001 that it does not understand, it will stop functioning within one minute, usually. The client application will no longer have access to Sabre or the gateway. The gateway application is unaffected by this vulnerability and all other users on the local system will continue to have connectivity.

DETAILS

Vulnerable systems:

* Sabre Desktop Reservation Software for Windows 4.2, 4.3, and 4.4

Background:

Sabre Inc.'s Desktop Reservation Software for Windows is a legacy travel agency program that has since been replaced by Sabre eVoya software.

However, several travel agencies and major airline travel call centers still use this software.

Securiteam: [NT] Denial of Service in Sabre Desktop Reservation Client for Windows

Analysis:

Local exploitation at an airline call center or travel agency could potentially slow or halt production. Under heavy load, the client will lock up, thereby forcing a reboot. This causes a loss of productivity, particularly in a high-volume call center. Automated ticketing systems running this client can be crashed as well. Since some companies using this software may not regularly monitor such events, they could miss ticketing deadlines, thereby having to pay out of pocket for ticket price changes or penalties

Recovery:

Restarting the application should restore normal functionality.

Vendor fix/Response:

Sabre responded with the following statement:

"Sabserv will be updated to ignore data it does not understand as part of the next maintenance upgrade to Sabre Desktop Reservation Software for Windows. This will prevent the denial of service condition within the client application when arbitrary data is sent to port 1001."

Disclosure Timeline:

- 07/26/2002 Issue disclosed to iDEFENSE
- 08/26/2002 Disclosed to vendor via e-mail to support@sabre.com
- 08/26/2002 Disclosed to iDEFENSE clients
- 09/03/2002 Second attempt at e-mail contact
- 09/15/2002 Call to Sabre technical support rep N2H, referred to customer support representative
- 09/20/2002 Fourth attempt at contact (leslie.price@sabre.com)
- 09/23/2002 Response received from Leslie Price
- 09/23/2002 Response received from Jeff Harmon (jeff.harmon@sabre.com)
- 10/10/2002 Coordinated public disclosure

ADDITIONAL INFORMATION

The original advisory can be downloaded by going to:

<<http://www.idefense.com/advisory/10.16.02.txt>>
<http://www.idefense.com/advisory/10.16.02.txt>

The information has been provided by <<mailto:dendler@idefense.com>> David Endler of iDEFENSE and <<mailto:adame780@bellsouth.net>> Altomo for finding the vulnerability.

=====

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

=====

=====

Securiteam: [NT] Denial of Service in Sabre Desktop Reservation Client for Windows

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: "[NT] Internet Explorer : The D-Day"
- **Messages sorted by:** [\[date \]](#) [\[thread \]](#) [\[subject \]](#) [\[author \]](#) [\[attachment \]](#)