

[NT] RAV Online Scanning ActiveX Buffer Overflow

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2003-07/0074.html>

From: SecuriTeam (support_at_securiteam.com)

Date: 07/20/03

To: list@securiteam.com

Date: 20 Jul 2003 19:50:54 +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

Beyond Security in Canada

Toronto-based Sunrays Technologies is now Beyond Security's representative in Canada.

We welcome ISPs, system integrators and IT systems resellers

to promote the most advanced vulnerability assessment solutions today.

Contact us at 416-482-0038 or at canadasales@beyondsecurity.com

RAV Online Scanning ActiveX Buffer Overflow

SUMMARY

<<http://www.ravantivirus.com/index.php>> RAV Online Scanning is "a free antivirus scanner for internet users. It is run on the user's browsers as an ActiveX".

The ActiveX file called ravonline.dll has a function named browseForFolder() that can be overflowed by passing a very long string as an argument. Since the function browseForFolder() is imported from Shell32.dll, so it looks like the problem maybe lay in the Shell32.dll and not in the ActiveX itself however users that use RAV Online Scanning are still vulnerable to the overflow.

DETAILS

Workaround:

Delete the ActiveX (ravonline.dll) in the "Downloaded Program Files" in your Windows Directory.

Vendor status:

Securiteam: [NT] RAV Online Scanning ActiveX Buffer Overflow

The vendor has been notified of the issue, no response have been received until now.

ADDITIONAL INFORMATION

The information has been provided by <mailto:trihuynh@zeeup.com> Tri Huynh.

=====

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.