

[NT] Multiple Vulnerabilities in the AtHoc Toolbar for MSIE

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2005-01/0103.html>

From: SecuriTeam (*support_at_securiteam.com*)

Date: 01/23/05

To: list@securiteam.com

Date: 23 Jan 2005 16:52:03 +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>

Multiple Vulnerabilities in the AtHoc Toolbar for MSIE

SUMMARY

Multiple vulnerabilities have been discovered in the <<http://www.athoc.com/site/products/toolbar.asp>> AtHoc toolbar that allows remote code execution through Internet Explorer when browsing to a specially crafted webpage. AtHoc sell a development suite which can allow a vendor to use their technology to create custom toolbars for their own clients.

Among the most renowned of AtHoc's toolbar clients are:

- * eBay
- * Accenture
- * ThomasRegister
- * ThomasRegional
- * Juniper Networks
- * WiredNews
- * CarFax
- * Agile PLM

DETAILS

Securiteam: [NT] Multiple Vulnerabilities in the AtHoc Toolbar for MSIE

The AtHoc toolbar comes with ActiveX component which exports a number of methods relating to the specifics of toolbar, such a skin settings, whether a debug log is to be kept, and numerous other options relating to customization.

When attempting to provide an overly long 'skin name' to the SetSkin() method exported by the control, a stack based buffer overflows, overwriting a saved return address on the stack and eventually allowing arbitrary code to be executed.

When the AtHoc toolbar is closed and re-started, a debug log is written containing various pieces of information relating to the success of certain operations which have been performed on the AtHoc toolbar during the users browsing session. One of the operations which is logged, is the setting of a 'base url', a value which is used by the toolbar when constructing absolute URLs for certain web related functionality. The SetBaseURL() function is used to set the base URL.

If the url provided to the function is not valid, the URL is logged by the toolbar in the debug log, which is stored in the root of the drive on which the toolbar is installed. The code which writes the invalid base URL to the debug log is vulnerable to a format string attack which can overwrite arbitrary dwords in memory with arbitrary values. It is possible to overwrite saved return addresses, function pointers, string pointers and more to easily gain control over the execution flow of the process, thus allowing arbitrary code execution.

The vulnerable component is marked safe for scripting by default, thereby allowing the dangerous functionality to be accessed with little user interaction.

Fix Information:

AtHoc has fixed these vulnerabilities and has advised the various vendors to update their toolbars to use the latest components. These fixed toolbars can be downloaded from the vendors respective websites.

ADDITIONAL INFORMATION

The information has been provided by <mailto:nisr@nextgenss.com>

NGSSoftware Insight Security Research.

The original article can be found at:

<<http://www.ngssoftware.com/advisories/athoc-01full.txt>>

<http://www.ngssoftware.com/advisories/athoc-01full.txt>

=====

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] Multiple Vulnerabilities in the AtHoc Toolbar for MSIE

=====
=====

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.