

[NT] WebArchiveX Unsafe Methods Vulnerability

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2005-09/0031.html>

From: SecuriTeam (support_at_securiteam.com)

Date: 09/08/05

To: list@securiteam.com

Date: 8 Sep 2005 10:33:41 +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>

WebArchiveX Unsafe Methods Vulnerability

SUMMARY

The <<http://www.csystems.co.il/webarchivex/index.aspx>> WebArchiveX component gives developers the ability to include .MHT archive creation in their software and is compatible with a wide range of programming languages.

Prior to September 6th 2005, the WebArchiveX ActiveX component would install and mark itself 'safe for scripting'. The component offers various methods that when instantiated by a malicious web site, can be used to read files from, or write files to the local computer.

DETAILS

The component has an extensive API that can be viewed online:

<<http://www.csystems.co.il/WebArchiveX/help/api.html>>

<http://www.csystems.co.il/WebArchiveX/help/api.html>

This advisory concentrates on the two following methods;

* MakeArchive – Build MHT web archive (single MHT file)

Boolean MakeArchive(
String htmlFile,

String htmlFile,

Securiteam: [NT] WebArchiveX Unsafe Methods Vulnerability

```
String userAgent,  
String mhtFile  
);
```

The MakeArchive method will accept a local path as the mhtFile parameter, allowing a malicious web site to write a file to the local drive. By writing to the startup folder, it is possible to create a .mht that will be executed locally at startup.

```
* MakeArchiveStr – Build MHT web archive and returns it as a string  
String MakeArchiveStr(  
    String htmlFile,  
    String userAgent  
);
```

The MakeArchiveStr method will accept a local path as the htmlFile parameter. After reading in the file, the contents will be returned to the calling script. This allows a malicious website to read the contents of any file accessible by the current user.

Solutions:

* The vendor has changed the default installation to remove the 'safe for scripting' entry, but unfortunately has not changed the version number. The download now includes a readme file that contains;

Why WebArchiveX is not safe for scripting?

If WebArchiveX was safe for scripting, then malicious websites could use WebArchiveX in order to read/write files from/to your local file system. Please contact support@csystems.co.il for further details!

In order to make WebArchiveX safe for scripting you can import the enclosed Registry file WebArchiveX_SafeForScripting.reg.

* To identify if this component is installed on your pc, search the registry for WebArchiveX entries.

* If the entry is located, remove the 'safe for scripting' entry by removing these keys;

```
\\Implemented Categories\\{7DD95801-9882-11CF-9FA9-00AA006C42C4}  
\\Implemented Categories\\{7DD95802-9882-11CF-9FA9-00AA006C42C4}
```

* For additional help contact support@csystems.co.il

ADDITIONAL INFORMATION

The information has been provided by
<mailto:brett.moore@security-assessment.com> Brett Moore.

Securiteam: [NT] WebArchiveX Unsafe Methods 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

=====

=====

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.