Vulnerability Advisory

Name	WebArchiveX - Unsafe Methods Vulnerability
Vendor Website	http://http://www.csystems.co.il/webarchivex/index.aspx
Date Released	September 07, 2005
Affected Software	WebArchiveX.dll 5.5.0.76 Installed Prior To Sep 6th, 2005
Researcher	Brett Moore brett.moore@security-assessment.com

Description

The 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 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.

Exploitation

The component has an extensive API that can be viewed online;
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 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.

Solution

- 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

About Security-Assessment.com

Security-Assessment.com is a leader in intrusion testing and security code review, and leads the world with SA-ISO, online ISO17799 compliance management solution. Security-Assessment.com is committed to security research and development, and its team have previously identified a number of vulnerabilities in public and private software vendors products.

For further information on this issue or any of our service offerings, contact us

Web www.security-assessment.com
Email info@security-assessment.com
Phone +649 302 5093