

[NT] MSIE May Download and Run Programs Automatically

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2001-12/0098.html>

From: support@securiteam.com

Date: 12/23/01

From: support@securiteam.com

To: list@securiteam.com

Date: Sun, 23 Dec 2001 04:40:06 +0100 (CET)

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

When was the last time you checked your server's security?

How about a monthly report?

<http://www.AutomatedScanning.com> -- Know that you're safe.

MSIE May Download and Run Programs Automatically

SUMMARY

Due to a flaw in the way Microsoft Internet Explorer handles certain HTTP reply strings, a web site can spoof the name of a file being requested and disguise it as a harmless file. A variation of this exploit may cause the browser to download and run a program file automatically without any user interaction or decision. This may lead to system compromise when visiting a malicious web site or opening an HTML mail message which directs the user to such site. Opening an e-mail attachment or accepting a file download is NOT required.

With some versions of IE, the origin web server of the file being downloaded can also be hidden by using a variation of this exploit. In this case it will show an empty string instead of the host name in the download dialog.

DETAILS

Vulnerable systems:

IE File ext Bypassing Hiding file

Version spoofing all dialogs origin

Securiteam: [NT] MSIE May Download and Run Programs Automatically

IE 6 yes yes no
IE 5.5 SP2 yes no? yes
IE 5.5 yes yes yes
IE 5.0 yes yes

The problem is in the way Internet Explorer handles the Content-type and Content-disposition HTTP headers of a web server reply. With certain combinations of specially crafted reply strings, the browser can be made first to start downloading the file without asking for confirmation from the user, and then to open it – or in this case, run it.

The same method that can mislead the user in the "plain" file name spoof variation of the attack can be used to mislead the browser's logics resulting in automatic execution of the program.

Workarounds:

If the patch cannot be applied for some reason, disabling file downloads from Tools -> Internet options -> Security -> Custom level -> Downloads/File download seems to stop the exploit. No other known workarounds exist now, except from switching to another browser such as Opera or Netscape, which do not seem to suffer from this problem.

Vendor status:

Microsoft was initially contacted on November 19 with the information regarding the "file extension spoofing" problem. The Security Warning dialogs of IE5 could be bypassed with that exploit, but the "automatically start an .exe" variation of the vulnerability was not known at the time. Microsoft did not consider the file extension-spoofing problem a security vulnerability. The company was informed about the new variation on November 27 and started working on a patch to correct the flaw. The patch is now out and downloadable on Microsoft's site at.

Patch:

The patch is available at:

<<http://www.microsoft.com/technet/security/bulletin/MS01-058.asp>>
<http://www.microsoft.com/technet/security/bulletin/MS01-058.asp>

Example (Exploit):

```
package nl.xs4all.kuperus.exploits;  
import javax.servlet.http.HttpServlet;  
import javax.servlet.http.HttpServletRequest;  
import javax.servlet.http.HttpServletResponse;  
import javax.servlet.ServletException;  
import java.io.IOException;  
import java.io.PrintWriter;
```

```
public class SpoofIt extends HttpServlet {
```

```
    protected void doGet(HttpServletRequest request, HttpServletResponse  
response) throws ServletException, IOException {
```

Securiteam: [NT] MSIE May Download and Run Programs Automatically

```
response.setContentType("application/hta");
response.setStatus(201);

PrintWriter out = response.getWriter();
out.write("this is a hta");

}

protected void doPost(HttpServletRequest request,
HttpServletResponse response) throws ServletException, IOException {
    super.doGet(request, response);
}
}
```

Once the user clicks on open, the HTA file is started according to its mime type Application/HTA. All the time the user is thinking it is actually a .txt file.

A working example is available at:
<<http://kuperus.xs4all.nl/microsoft.txt>>
<http://kuperus.xs4all.nl/microsoft.txt>

ADDITIONAL INFORMATION

The information has been provided by <<mailto:jouko@solutions.fi>> Jouko Pynnonen and <<mailto:jelmer@kuperus.xs4all.nl>> jelmer.

=====

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.

-
- **Previous message:** support@securiteam.com: "[UNIX] POPAuth Symlink Problem Allows Creation of a Setuid Shell"
 - **Messages sorted by:** [\[date \]](#) [\[thread \]](#) [\[subject \]](#) [\[author \]](#) [\[attachment \]](#)