

Security bug in .NET Forms Authentication

Source: <http://www.derkeiler.com/Mailing-Lists/NT-Bugtraq/2004-09/0068.html>

From: Toby Beaumont (*toby_at_CREATOR.CO.UK*)

Date: 09/14/04

Date: Tue, 14 Sep 2004 12:42:28 +0100

To: NTBUGTRAQ@LISTSERV.NTBUGTRAQ.COM

Hi

We believe we have discovered a serious flaw in .NET forms authentication when used to secure sub folders.

A standard forms authentication setup requires the presence of "web.config" to set the authentication method and login procedure. The presence of this file prevents access to certain files (.aspx files for example) unless authenticated.

Example

The webroot for your website is:

c:\inetpub\wwwroot\mysite

You want to secure files in a sub directory "secure"

c:\inetpub\wwwroot\mysite\secure\web.config

A request to <http://localhost/secure/somefile.aspx> would then redirect the user to a predefined authentication page, as defined in web.config, before allowing the user access to "somefile.aspx".

Bug

1. Using Mozilla not IE, you make a request to <http://localhost/secure\somefile.aspx> The use of a backslash rather than a forward slash appears to bypass the expected authentication model invoked in .NET forms authentication

2. Using IE, you make a request to <http://localhost/secure\somefile.aspx> - IE automatically replaces the backslash "\" with a forward slash "/" and everything appears fine. However, replace the backslash "\" with %5C (%5C being hex value for \) and all is not so fine:

<http://localhost/secure%5Csomefile.aspx>

Interestingly (and I guess now somewhat amusingly) Microsoft point out in the article "Design Guidelines for Secure Web Applications"

NT-Bugtraq: Security bug in .NET Forms Authentication

(<http://msdn.microsoft.com/library/default.asp?url=/library/en-us/dnnetsec/html/THCMCh04.asp>):

"Be Careful with Canonicalization Issues:

Data in canonical form is in its most standard or simplest form. Canonicalization is the process of converting data to its canonical form. File paths and URLs are particularly prone to canonicalization issues and many well-known exploits are a direct result of canonicalization bugs. For example, consider the following string that contains a file and path in its canonical form."

And then goes on to define the exploit ;-)

(Russ - I have not posted this message anywhere as yet, nor have I contacted Microsoft. If you indeed confirm this exploit, you are the first to know).

Regards,

==

Toby Beaumont

Director of Technology

Creator

This email and any attached files are for the exclusive use of the addressee and may contain privileged and/or confidential information. If you receive this email in error you should not disclose the contents to any other person nor take copies but should delete it and telephone us immediately.

Creator makes no warranty as to the accuracy or completeness of this email and accepts no liability for its contents or use. Any opinions expressed in this email are those of the author and do not necessarily reflect the opinions of Creator.

If you or your employer does not consent to the receipt of emails of this kind then please notify us immediately.

Creator

4 Grafton Mews

London

W1T 5JE

United Kingdom

Tel: 020 7391 5151

DDI: 020 7391 5128

Fax: 020 7391 5152

Web: <http://www.creator.co.uk>

NTBugtraq Editor's Note:

Want to reply to the person who sent this message? This list is configured such that just hitting
