

[NEWS] IBM Net.Data Internal Variables Display Vulnerability

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2003-01/0021.html>

From: support@securiteam.com

Date: 01/05/03

From: support@securiteam.com

To: list@securiteam.com

Date: 6 Jan 2003 00:11:02 +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

Beyond Security would like to welcome Tiscali World Online to our service provider team.

For more info on their service offering IP-Secure, please visit http://www.worldonline.co.za/services/work_ip.asp

IBM Net.Data Internal Variables Display Vulnerability

SUMMARY

Net.Data is a full-featured and easy to learn scripting language that allows you to create powerful Web applications. A security vulnerability in the product allows attackers to view internal variables values, which may disclose sensitive information such as pathnames, server names, usernames and passwords.

DETAILS

A HTML form that accepts user input, and displays this input back to the user, can be maliciously exploited by typing in the form the variable name.

Some variables are predefined in Net.Data, and potentially damaging.

\$(DTW_CURRENT_FILENAME) always contains the internal script name and full path.

If the database server is different from the application server, then

\$(DATABASE) , \$(LOGIN), and \$(PASSWORD) must be defined and contain the connection parameters.

Securiteam: [NEWS] IBM Net.Data Internal Variables Display Vulnerability

If the Net.Data script displays back the information passed to it, and an attacker passes the string \$(LOGIN) as the form content, the resulting HTML will display the connection profile.

Other predefined variables may be found at:

<<http://www-3.ibm.com/software/data/net.data/docs/noframes/db2rn/index.htm>>

<http://www-3.ibm.com/software/data/net.data/docs/noframes/db2rn/index.htm> (Language Environment Variables and Miscellaneous Variables).

The problem is not limited to predefined variables. Any variable can be retrieved, if you know its name. This provides an interesting backdoor for developers (and ex-developers..)

Workaround:

You cannot avoid showing internal variables, but you can reduce the risk from the database connection exposure. Rewrite the Net.Data application so all remote database access goes through local programs rather than directly from the script.

Vendor's Response:

The bug has been posted on the Net.Data IBM managed forum, And on another user forum, which is monitored by IBM. No response was received.

ADDITIONAL INFORMATION

The information has been provided by <mailto:shalom@venera.com> Shalom Carmel.

=====

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.