

[NEWS] IBM Net.Data Macro Name Cross-Site Scripting Vulnerability

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2004-01/0083.html>

From: SecuriTeam (support_at_securiteam.com)

Date: 01/28/04

To: list@securiteam.com

Date: 28 Jan 2004 17:37:40 +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 Net.Data Macro Name Cross-Site Scripting Vulnerability

SUMMARY

" <<http://www-3.ibm.com/software/data/net.data/>> Net.Data, a full-featured and easy to learn scripting language, allows you to create powerful Web applications. Net.Data can access data from the most prevalent databases in the industry".

A vulnerability has been identified in IBM Net.Data which can be used by attackers to conduct cross-site scripting attacks.

DETAILS

Vulnerable Systems:

* IBM Net.Data version 7 and 7.2, possibly prior

The vulnerability is caused due to an input validation error in the db2www CGI component, since the name of a requested macro file is included in "DTWP001E" error messages without sufficient sanitation. This can be exploited by constructing a link which includes arbitrary script code. If a user is tricked into clicking the link or visiting a malicious website, the script code will be executed in the user's browser session in context

Securiteam: [NEWS] IBM Net.Data Macro Name Cross-Site Scripting Vulnerability

of the affected site.

Example:

```
http://[victim]/cgi-bin/db2www/<scr!pt>alert(document.domain)</scr!pt>
```

(note the word "script" has been replaced with "scr!pt")

Successful exploitation may result in disclosure of various information (e.g. cookie-based authentication information) associated with the site running IBM Net.Data, or inclusion of malicious content which the user thinks is part of the real website. Other error messages may also be affected.

Workaround

The vendor recommends that the "DTW_DEFAULT_ERROR_MESSAGE" feature (or "DTW_DEFAULT_MACRO" feature on zOS and iServer) is used to ensure that a web site reacts in a predictable manner when encountering problems.

In the Net.Data configuration file "db2www.ini", insert an entry such as:

```
DTW_DEFAULT_ERROR_MESSAGE This Web Site is experiencing problems.  
Check back later.
```

This will prevent various error messages from being returned to users.

Time Table

- * 04/11/2003 – Vulnerability discovered
- * 04/11/2003 – Vendor notified
- * 07/11/2003 – Vendor confirms receiving vulnerability report. Report will be forwarded to Net.Data team
- * 02/12/2003 – Requests status report from contact person
- * 02/12/2003 – Contact person responds that the Net.Data team will be contacted
- * 14/01/2004 – Advisory draft sent to vendor along with set disclosure date
- * 14/01/2004 – Contact person replies that the Net.Data team will be contacted again
- * 22/01/2004 – Vendor confirms vulnerability and provides solution
- * 26/01/2004 – Public disclosure

ADDITIONAL INFORMATION

The information has been provided by <mailto:che@secunia.com> Carsten H. Eiram

=====

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

Securiteam: [NEWS] IBM Net.Data Macro Name Cross-Site Scripting Vulnerability

=====
=====

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.