

[NT] NetCharts XBRL Server Information Leakage Vulnerability

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2003-02/0049.html>

From: support@securiteam.com

Date: 02/17/03

From: support@securiteam.com

To: list@securiteam.com

Date: 17 Feb 2003 22:43:33 +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

NetCharts XBRL Server Information Leakage Vulnerability

SUMMARY

<<http://www.visualmining.com/>> NetCharts XBRL Server is a data visualization service that generates charts and graphs, tables, and reports. It can be used alone or in conjunction with any web infrastructure from the simplest CGI scripts to the most sophisticated Enterprise Application Server. A vulnerability in the product allows an attacker sending a malformed-chunked encoding request to cause the server to reveal sensitive information about itself.

DETAILS

Vulnerable systems:

- * NetCharts XBRL Server v4.0.0 for Windows 2000

A client may connect to the target machine and deliver several requests with an invalid chunked encoded body.

The potential for information leakage is not great but the risk is mitigated somewhat by the unpredictability of the query-response de-synchronization. Depending on the target site, this may be somewhat exploitable by a malicious user to redirect other users to a specific

Securiteam: [NT] NetCharts XBRL Server Information Leakage Vulnerability

response by saturating the communication channels with a desired response.

Example:

===== SNIP =====

GET /index.jsp HTTP/1.1
Host: victim.com
Transfer-Encoding: Chunked

53636f7474

===== SNIP =====

ADDITIONAL INFORMATION

The information has been provided by <mailto:ts@securityoffice.net> Tamer Sahin.

=====

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.