

[NT] DirectContact Directory Traversal

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2006-03/msg00018.html>

- *From:* SecuriTeam <support@xxxxxxxxxxxxxx>
 - *Date:* 7 Mar 2006 19:36:18 +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>

DirectContact Directory Traversal

SUMMARY

<<http://revero.info/dc/>> DirectContact "turns your computer in real "friendly" HTTP server." The DirectContact program is unable to manage malicious patterns like ..\ or ../, allowing an attacker can go out the document root assigned to the webserver and see/download all the files available on the remote system.

DETAILS

Vulnerable Systems:
* DirectContact version 0.3b

Proof of concept:
To test the vulnerability:

Via browser:
[http://\[host\]:\[port\]/..\..\..\windows/system.ini](http://[host]:[port]/..\..\..\windows/system.ini)

Via raw request:
GET ../../../../windows/system.ini HTTP/1.1

ADDITIONAL INFORMATION

The information has been provided by <<mailto:fdonato@xxxxxxxxxxxxxx>>
Donato Ferrante.

The original article can be found at:

<<http://www3.autistici.org/fdonato/advisory/DirectContact0.3b-adv.txt>>

<http://www3.autistici.org/fdonato/advisory/DirectContact0.3b-adv.txt>

=====

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@xxxxxxxxxxxxxx

In order to subscribe to the mailing list, simply forward this email to: list-subscribe@xxxxxxxxxxxxxx

=====

=====

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.