

[NT] ASUS Remote Console Buffer Overflow

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2008-03/msg00075.html>

- *From:* SecuriTeam <support@xxxxxxxxxxxxxx>
 - *Date:* 31 Mar 2008 13:24:00 +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>

ASUS Remote Console Buffer Overflow

SUMMARY

"The <<http://www.asus.com/999/html/share/9/icon/9/index.htm#asmb3>> ASUS Remote Console (ARC) is an efficient and flexible application that allows monitoring and control of the remote host." The main component of this service is a telnet server listening on port 623 which is called DpcProxy and provides an IPMI interface. A buffer overflow vulnerabilities has been discovered in the ASUS remote console.

DETAILS

Vulnerable Systems:

- * ASUS Remote Console version 2.0.0.24

The DPC Proxy is affected by a buffer-overflow vulnerability located in the function which gets the data received from the client, stores them in a stack buffer of about 1024 bytes and checks the presence of an end of line delimiter (carriage return).

ADDITIONAL INFORMATION

[NT] ASUS Remote Console Buffer Overflow

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

The original article can be found at:

<<http://alugi.altervista.org/adv/asuxdpc-adv.txt>>

<http://alugi.altervista.org/adv/asuxdpc-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@xxxxxxxxxxxxx

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

=====

=====

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.