

[NEWS] Packeteer PacketShaper Predictable TCP ISN

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2007-05/msg00033.html>

- *From:* SecuriTeam <support@xxxxxxxxxxxxxx>
 - *Date:* 21 May 2007 10:30:54 +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>

Packeteer PacketShaper Predictable TCP ISN

SUMMARY

Packeteer PacketShaper has been found to be vulnerable to a vulnerability that allows remote attackers to predict the next ISN number that will be given by the TCP stack.

DETAILS

Vulnerable Systems:

- * Packeteer PacketShaper versions 7.3.0g2 and 7.5.0g1

The TCP/IP stack of Packeteer PacketShaper is generating predictable initial sequence numbers (ISN): The sequence number is incremented by 128000 per second and by 64000 per connection. (As an example, if the current SYN/ACK ISN is 319104000 then about six seconds later the ISN is likely to be 319936000.) This allows an attacker to spoof connections from trusted clients or launch a DoS attack.

ADDITIONAL INFORMATION

[NEWS] Packeteer PacketShaper Predictable TCP ISN

The information has been provided by <<mailto:nnposter@xxxxxxxxxxxxxx>>
nnposter.

=====

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.