

[TOOL] Komahayown, Inverse Connection Remote Shell

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2003-05/0077.html>

From: SecuriTeam (*support_at_securiteam.com*)

Date: 05/31/03

To: list@securiteam.com

Date: 31 May 2003 12:16:04 +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

In the US?

Contact Beyond Security at our new California office housewarming rates on automated network vulnerability scanning. We also welcome ISPs and other resellers!

Please contact us at: 323-882-8286 or ussales@beyondsecurity.com

Komahayown, Inverse Connection Remote Shell

DETAILS

Komahayown is a shellcode and client for remote execution of commands through an inverse connection (using random ports using the TCP protocol).

Such an inverse channel is needed because in most cases a Firewall will block incoming ports to a server, but will be a lot less restrictive on outgoing connections. By creating such an inverse channel, an attacker can cause the shellcode to run commands (by sending a simple ICMP packet), and send back the response via an unrestricted TCP port.

A diagram illustrating the mechanism can be viewed by going to:

<http://www.shellcode.com.ar/st0xff/kmh_wflow.jpg>

http://www.shellcode.com.ar/st0xff/kmh_wflow.jpg

ADDITIONAL INFORMATION

The tool can be downloaded from:

<<http://www.shellcode.com.ar/en/proyectos.html>>

Securiteam: [TOOL] Komahayown, Inverse Connection Remote Shell

<http://www.shellcode.com.ar/en/proyectos.html>

The information has been provided by ">Matias Sedalo.

=====

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.