

[TOOL] ISH Detection Tool

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2002-01/0133.html>

From: support@securiteam.com

Date: 01/29/02

From: support@securiteam.com

To: list@securiteam.com

Date: Tue, 29 Jan 2002 22:24:24 +0100 (CET)

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

When was the last time you checked your server's security?

How about a monthly report?

<http://www.AutomatedScanning.com> -- Know that you're safe.

ISH Detection Tool

DETAILS

ISH Detect is a tool that is able to detect the presence (off the wire) of the product of ICMP Shell.

<<http://www.securiteam.com/tools/5PP0M0K60O.html>> ICMP Shell is a program written in C for the UNIX environment that allows an administrator to access their computer remotely via ICMP packets.

ICMP Shell uses an identifier of 16 bits in each ICMP packet to communicate between the client and the server. ISH Detect tries to detect the presence of the ICMP Shell by sending ICMP packets while varying the identifier from 0 to 65535 and watching for the response. If the server receives a package with a bad identifier, it will not answer (unlike normal operating system behavior).

ADDITIONAL INFORMATION

The tool can be downloaded from:

<http://www.securiteinfo.com/download/ish_detect.tgz>

http://www.securiteinfo.com/download/ish_detect.tgz

The information has been provided by <<mailto:commercial@securiteinfo.com>>
Eyrill / Securiteinfo.com.

Securiteam: [TOOL] ISH Detection Tool

=====
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.

- **Previous message:** support@securiteam.com: "[EXPL] SHOUTcast Vulnerable to Malformed CGI Request (admin.cgi)"
- **Messages sorted by:** [\[date \]](#) [\[thread \]](#) [\[subject \]](#) [\[author \]](#) [\[attachment \]](#)