

[UNIX] Multiple Vendor "talkd" User Validation Fault

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2002-04/0011.html>

From: support@securiteam.com

Date: 04/04/02

From: support@securiteam.com

To: list@securiteam.com

Date: Thu, 4 Apr 2002 11:53:18 +0200 (CEST)

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.

Multiple Vendor "talkd" User Validation Fault

SUMMARY

"talk" is a program available on multiple UNIX OSs that allows users to communicate within a system and/or remotely. There exists a flaw within the "talkd" which allows anyone masquerade as anyone else either remotely or within the confines of the system. This is due to the lack of user validation by the "talkd" for incoming "talk" requests. This may be a catalyst for social engineering that can lead to the revealing of private or sensitive information from other users.

DETAILS

Identification of User Masquerading

If someone is initiating a talk request with "talksp00f" from the user "root" for example. You should check to see if the root user is actually logged in. And if he is not you can monitor the system processes and figure out who is initiating the bogus talk request.

Also, if the user that is supposedly initiating the talk request to you **is** logged in. Check that users processes to see if he is actually initiating the talk request to you.

Securiteam: [UNIX] Multiple Vendor "talkd" User Validation Fault

Exploitation:

The exploit code can be downloaded from:

<<http://www.superw00t.com/projects/talkspooof.tar.gz>>

<http://www.superw00t.com/projects/talkspooof.tar.gz>

ADDITIONAL INFORMATION

The information has been provided by <<mailto:tek@superw00t.com>> Tekno
pHReak.

=====

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: "[NEWS] Netware Remote Manager Found to Contain a Buffer Overflow"
 - **Messages sorted by:** [\[date \]](#) [\[thread \]](#) [\[subject \]](#) [\[author \]](#) [\[attachment \]](#)