

[UNIX] Confirm Command Execution Vulnerability

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2004-02/0081.html>

From: SecuriTeam (support_at_securiteam.com)

Date: 02/26/04

To: list@securiteam.com

Date: 26 Feb 2004 11:48:16 +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>

Confirm Command Execution Vulnerability

SUMMARY

<<http://freshmeat.net/projects/confirm/>> Confirm is "a simple procmail script that uses a pattern-matching auto-whitelist to help identify unsolicited email". A critical security flaw was found in Confirm 0.62 and below that allows a remote user to craft a unique e-mail that will execute a command on the local system using the credentials of the user running confirm.

DETAILS

Vulnerable Systems:

- * Confirm version 0.62 and prior

Immune Systems:

- * Confirm version 0.70

Due to insufficient user supplied data filtering, emails containing special characters, like ";,|,,\$ and so on in headers trick Confirm and lead to command execution.

How to patch:

Install confirm-0.70 from:

Securiteam: [UNIX] Confirm Command Execution Vulnerability

<<http://hr.uoregon.edu/davidrl/confirm/confirm-0.70.tgz>>
<http://hr.uoregon.edu/davidrl/confirm/confirm-0.70.tgz>.

ADDITIONAL INFORMATION

The information has been provided by <mailto:emsi@GTS.PL> Mariusz Woloszyn.

=====

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.