

[UNIX] CMU SNMP Utilities snmptrad Format String

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2006-01/msg00095.html>

- *From:* SecuriTeam <support@xxxxxxxxxxxxxxx>
 - *Date:* 30 Jan 2006 10:52:25 +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>

CMU SNMP Utilities snmptrad Format String

SUMMARY

The package is <<http://www.gaertner.de/snmp/>> CMU-SNMP utilities. "In this package snmptrapd is an SNMP application that receives and logs SNMP TRAP and INFORM messages. This daemon by default is to listen on UDP port 162 on all IPv4 interfaces. Since 162 is a privileged port, snmptrapd must typically be run as root".

There is a format string vulnerability in the snmptrapd server from the cmu-snmp package.

DETAILS

Vulnerable Systems:

- * snmptrapd (cmu-snmp-linux-3.7 package)
- * snmptrapd (cmu-snmp-linux-3.6 package)

The vulnerability persist in the snmp_input() function. An attacker could abuse this vulnerability from remote while sending specially crafted packets. Successful exploitation consist in arbitrary code execution, with root privileges by default.

Disclosure Timeline:

22.12.05 – First notification.

09.01.06 – Second notification.

ADDITIONAL INFORMATION

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

The original article can be found at:

<<http://www.digitalarmaments.com/2006040164883273.html>>

<http://www.digitalarmaments.com/2006040164883273.html>

=====

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.

- Prev by Date: [*\[REVS\] Cross Site Cooking*](#)
- Next by Date: [*\[NT\] Cerberus FTP Server DoS \(CVH, Exploit\)*](#)
- Previous by thread: [*\[REVS\] Cross Site Cooking*](#)
- Next by thread: [*\[NT\] Cerberus FTP Server DoS \(CVH, Exploit\)*](#)
- Index(es):
 - ◆ [*Date*](#)
 - ◆ [*Thread*](#)