

[UNIX] SNMPd Log Files Buffer Overflow Problem

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2001-08/0053.html>

From: support@securiteam.com

Date: 08/11/01

From: support@securiteam.com

To: list@securiteam.com

Subject: [UNIX] SNMPd Log Files Buffer Overflow Problem

Message-Id: <20010811102639.75A31138BF@mail.der-keiler.de>

Date: Sat, 11 Aug 2001 12:26:39 +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>

SNMPd Log Files Buffer Overflow Problem

SUMMARY

<<http://sourceforge.net/projects/net-snmp/>> net-snmp provides tools and libraries relating to the Simple Network Management Protocol including: An extensible agent, an SNMP library, tools to request or set information from SNMP agents, tools to generate and handle SNMP traps, etc.

SNMPd suffers from a buffer overflow vulnerability that allows a local attacker to cause the program to execute arbitrary code.

DETAILS

Vulnerable systems:

ucd-snmp version 4.2.1 (Official)

Immune systems:

ucd-snmp version 4.2.1 (CVS)

SNMPd provides a parameter named '-l', this specifies which file should be used for logging. If SNMPd is lunched with an overly long argument (-l) of the sort: "-l AAAAAAAAAA...[455 chars]" the program will crash. This buffer overflow would allow a local attacker to execute arbitrary code.

Vulnerable code:

On line 306 of snmpd.c, they have:

```
char logfile[SNMP_MAXBUF_SMALL];
```

Where SNMP_MAXBUF_SMALL is defined in tools.h as a 512 buffer.

Securiteam: [UNIX] SNMPd Log Files Buffer Overflow Problem

And last but not least, on line 321 of snmpd.c:
strcpy(logfile, LOGFILE);

Solution:

An update has been posted to the CVS. Download the latest version from:

<<http://sourceforge.net/projects/net-snmp/>>

<http://sourceforge.net/projects/net-snmp/>

ADDITIONAL INFORMATION

The information has been provided by <<mailto:security@eds.com.ar>>
SECURITY and <<mailto:methodic@libpcap.net>> Tony Lambiris.

=====

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] Microsoft Passport Account Hijacking (Hacking Hotmail and more)"
 - **Messages sorted by:** [\[date \]](#) [\[thread \]](#) [\[subject \]](#) [\[author \]](#) [\[attachment \]](#)