

[UNIX] Sendmail Memory Leak DoS

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2006-03/msg00076.html>

- *From:* SecuriTeam <support@xxxxxxxxxxxxxxxx>
 - *Date:* 23 Mar 2006 14:19:44 +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>

Sendmail Memory Leak DoS

SUMMARY

<<http://www.sendmail.com/>> sendmail is "a powerful, efficient, and scalable Mail Transport Agent"

A memory leak in Sendmail allows attackers to DoS sendmail by exhausting memory.

DETAILS

Vulnerable Systems:

- * Sendmail version 8.13.5 and prior
- * Sendmail version 8.12.10 and prior

Immune Systems:

- * Sendmail version 8.13.6

The function `sm_syslog` at `conf.c` contain a memory leak.

The memory leak will cause with every be a usage of `sm_syslog`, allocation of new memory that will never be released, until all available memory has been exhausted.

[UNIX] Sendmail Memory Leak DoS

Code Snips:

File conf.c line 5324:

```
/* VARARGS3 */
void
#ifdef __STDC__
sm_syslog(int level, const char *id, const char *fmt, ...)
#else /* __STDC__ */
sm_syslog(level, id, fmt, va_alist)
..
for (;;)
{
int n;

/* print log message into buf */
SM_VA_START(ap, fmt);
n = sm_vsnprintf(buf, bufsize, fmt, ap);
SM_VA_END(ap);
SM_ASSERT(n > 0);
if (n < bufsize)
break;

/* String too small, redo with correct size */
bufsize = n + 1;
if (buf != buf0)
{
sm_free(buf);
buf = NULL;
}
buf = sm_malloc_x(bufsize);
}

/* clean up buf after it has been expanded with args */
newstring = str2prt(buf);
if ((strlen(newstring) + idlen + 1) < SYSLOG_BUFSIZE)
{
..
if (buf == buf0)
buf = NULL; <- Memory leak
errno = save_errno;
return;
}
```

Vendor Status:

The vendor has issued a fix: <<http://www.sendmail.org/8.13.6.html>>

<http://www.sendmail.org/8.13.6.html>

Patch for Sendmail version 8.13.5 available at:

<<ftp://ftp.sendmail.org/pub/sendmail/8.13.5.p0>>

<ftp://ftp.sendmail.org/pub/sendmail/8.13.5.p0>

Patch for Sendmail version 8.12.11 available at:

<<ftp://ftp.sendmail.org/pub/sendmail/8.12.11.p0>>

<ftp://ftp.sendmail.org/pub/sendmail/8.12.11.p0>

ADDITIONAL INFORMATION

The information has been provided by Ido Kanner (SecuriTeam).

=====

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.