

# [NEWS] ClamAV Library Multiple Heap Overflows (TNEF, CHM, FSG)

**Source:** <http://www.derkeiler.com/Mailing-Lists/Securiteam/2005-08/0028.html>

---

**From:** SecuriTeam ([support\\_at\\_securiteam.com](mailto:support_at_securiteam.com))

**Date:** 08/08/05

To: [list@securiteam.com](mailto:list@securiteam.com)

Date: 8 Aug 2005 13:20:31 +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>

-----

ClamAV Library Multiple Heap Overflows (TNEF, CHM, FSG)

---

## SUMMARY

<<http://www.clamav.net/>> ClamAV is "the most widely used GPL antivirus library today. It provides file format support for virus analysis". During the processing of TNEF, CHM, & FSG formats an attacker is able to trigger several integer overflows that allow attackers to overwrite heap data to obtain complete control of the system.

## DETAILS

### Vulnerable Systems:

- \* ClamAV Version 0.86.1 (current) and prior
- \* There are numerous implementations of ClamAV listed on their site which are likely vulnerable. One party to note is Apple. Apple includes ClamAV by default in Mac OS X Server. In addition, ClamAV has been ported to windows and a variety of other platforms by third parties who's implementations are also likely vulnerable. Refer to vendor for specifics.

### Immune Systems:

- \* ClamAV version 0.86.2 fixes some of the issues, specifically, the two integer overflows in TNEF.

## Securiteam: [NEWS] ClamAV Library Multiple Heap Overflows (TNEF, CHM, FSG)

### Vulnerable Code:

TNEF processing contains at least two integer overflows that result in a heap overflows. The following code from `tnef_attachment()` and `tnef_message()` in `tnef.c` is vulnerable. The `length` field is an arbitrary 32-bit integer. If `length` is `-1`, it will wrap and `malloc()` will return a small heap buffer which is overflowed on the following `fread()`.

```
string = cli_malloc(length + 1);
if(fread(string, 1, length, fp) != length) {
    free(string);
    return -1;
}
```

CHM processing contains an integer overflow that results in heap corruption. The following is vulnerable code from `read_chunk_entries()` in `chmunpack.c`. If `length` is `-1`, it will wrap and `malloc()` will return small heap buffer which is overflowed on the following `strncpy()`.

```
name_len = read_enc_int(&current, end);
file_e->name = (unsigned char *) cli_malloc(name_len+1);
if (!file_e->name) {
    free(file_e);
    return FALSE;
}
strncpy(file_e->name, current, name_len);
```

FSG processing contains a faulty boundary check that results in a buffer overflow. The following is vulnerable code from `unfsg()` in `fsg.c`. Specifically, `backbytes` and `backsize` are essentially encoded arbitrary 32-bit unsigned integers; and, if both are slightly negative values an attacker can trigger a heap overflow because of the integer wraps in the boundary check.

```
if (cdst-backbytes < dest || cdst+backsize >= dest+dszie)
return -1;
while(backsize-->) {
    *cdst=*(cdst-backbytes);
    cdst++;
}
```

### ADDITIONAL INFORMATION

The original article can be found at:

<http://www.rem0te.com/public/images/clamav.pdf>  
<http://www.rem0te.com/public/images/clamav.pdf>

=====

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](mailto:list-unsubscribe@securiteam.com)

Securiteam: [NEWS] ClamAV Library Multiple Heap Overflows (TNEF, CHM, FSG)

In order to subscribe to the mailing list, simply forward this email to: [list-subscribe@securiteam.com](mailto: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.