

[UNIX] mutt mutt_decode_xbit() Buffer Overflow

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2005-09/0038.html>

From: SecuriTeam (support_at_securiteam.com)

Date: 09/08/05

To: list@securiteam.com

Date: 8 Sep 2005 14:06:15 +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>

mutt mutt_decode_xbit() Buffer Overflow

SUMMARY

" <<http://www.mutt.org/>> Mutt is a small but very powerful text-based mail client for UNIX operating systems."

By sending a maliciously crafted email to the mutt program an attacker can cause the program to execute arbitrary code.

DETAILS

The problem is in the mutt attachment/encoding/decoding functions, specifically `handler.c:mutt_decode_xbit()` and the buffer `bufi[BUFI_SIZE]`.

The variable 'l' is used as a counter to reference a position in the buffer and under certain circumstances its value can be manipulated and becomes much larger than the size of this buffer, thus overwriting other memory with many possible consequences.

This counter should never exceed the size and I believe the logic in the `convert_to_state()` function is supposed to reset it to 0, however there is a flaw – There are other functions affected in the same way due to copy/paste, such as `mutt_decode_uuencoded()`.

Securiteam: [UNIX] mutt mutt_decode_xbit() Buffer Overflow

Proof of Concept :

Mutt buffer overflow POC.

Discovered by Frank Denis <j@42-networks.com>

-- snip snip --