From: nasoor bagheri <na.bagheri@gmail.com>
Sent: Saturday, May 25, 2019 6:34 AM
To: lwc-forum@list.nist.gov
Cc: sadegh sadeghi; Muhammad Reza Z'aba; cilipadi@cybersecurity.my; saufy@uitm.edu.my
Subject: [lwc-forum] OFFICIAL COMMENT: CiliPadi

Dear All,

In CiliPadi document, section 3.3, it is stated as follow:

"3.3 Padding
Both the associated data and message blocks are individually padded only if its
length is not a multiple of r bits. Padding is performed by adding a bit 1, and
then as many zero bits as necessary until the padded data is in multiple of r
bits. If the length of the last block is r - 1 bits, then only bit 1 is added."

Based on this padding approach, it CiliPadi vulnerable against length extension attack., e.g.,
E(M,K)=E(M||0x80), when M\in{0,1}^{r-8}. Bellow is an example of such a collision/fogeray with empty plaintext for the "Mild" version, based on their refrence source code:

Key = 000102030405068008090A0B0C0D0E80
Nonce = 000102030405068008090A0B0C0D0E80
PT =
AD = 00010203040506
Cipherext =
Tag= 158244EEA881F6C9

Key = 000102030405068008090A0B0C0D0E80
Nonce = 000102030405068008090A0B0C0D0E80
Plaintext =
AD = 0001020304050680
Cipherext =
Tag= 158244EEA881F6C9

Bellow is a forgery example with non-emphy plaintext

Count = 529
Key = 000102030405060708090A0B0C0D0E80
Nonce = 000102030405060708090A0B0C0D0E80
Plaintext = 000102030405060708090A0B0C0D0E80
AD =
Cipherext = 4A1EAAD2F68E41B3891A5632EC092000
Tag= CECA7773AC3434B7

Count = 496
Key = 000102030405060708090A0B0C0D0E80
Nonce = 000102030405060708090A0B0C0D0E80

Plaintext = 000102030405060708090A0B0C0D0E
AD =
Cipherext = 4A1EAAD2F68E41B3891A5632EC0920
Tag= CECA7773AC3434B7

However, it can be fixed easily by minor modification in the mode of operation. For example, to fix this problem, a padded and an unpadded message should be processed differently, e.g. by different masking in the capacity part, including the message/AD length in the process, or by using 10^* paddings for all messages.

PS1: The proposed attack works against all variants of CiliPadi, i.e., Mild, Medium, Hot and ExtraHot.

PS2: We appreciate the CiliPadi team that verified and confirmed our observation.

Best Regards,
Nasour Bagheri and Sadegh Sadeghi
--

From: Muhammad Reza Z'aba <muhdreza@gmail.com>
Sent: Saturday, May 25, 2019 1:27 PM
To: nasoor bagheri
Cc: lwc-forum@list.nist.gov; sadegh sadeghi; Muhammad Reza Z'aba; cilipadi@cybersecurity.my; saufy@uitm.edu.my
Subject: Re: [lwc-forum] OFFICIAL COMMENT: CiliPadi

Dear all,

We thank Nasour and Sadegh for pointing out the mistake in the specification of CiliPadi. We will issue an updated specification and source code as soon as possible in this forum.

Regards,
Reza.

On Sat, May 25, 2019 at 6:34 PM nasoor bagheri <na.bagheri@gmail.com> wrote:

> Dear All,
>
> In CiliPadi document, section 3.3, it is stated as follow:
>
> "3.3 Padding
> Both the associated data and message blocks are individually padded only if its
> length is not a multiple of r bits. Padding is performed by adding a bit 1, and
> then as many zero bits as necessary until the padded data is in multiple of r
> bits. If the length of the last block is r - 1 bits, then only bit 1 is added."
>
> Based on this padding approach, it CiliPadi vulnerable against length extension attack., e.g., E(M,K)=E(M||0x80), when M\in{0,1}^{r-8}. Bellow is an example of such a collision/fogeray with empty plaintext for the "Mild" version, based on their refrence source code:
>
> Key = 000102030405068008090A0B0C0D0E80
> Nonce = 000102030405068008090A0B0C0D0E80
> PT =
> AD = 00010203040506
> Cipherext =
> Tag= 158244EEA881F6C9
>
> Key = 000102030405068008090A0B0C0D0E80
> Nonce = 000102030405068008090A0B0C0D0E80
> Plaintext =
> AD = 0001020304050680
> Cipherext =
> Tag= 158244EEA881F6C9
>
> Bellow is a forgery example with non-emphy plaintext
>
> Count = 529
> Key = 000102030405060708090A0B0C0D0E80