Dear All,

It seems syconaer96128v1 will output same Tag for two packets in some cases if the only differences are in the last bytes of Associated Data D and the values are 80(00) and 00(00).

It seems there are also collisions in some cases with Associated Data tails being 0x8080, 0x0180, 0x0080.

I was not able to reproduce it for syconaer64128v1.

Best regard,

Alexandre Mege

Ex for syconaer96128v1

Key = 000102030405060708090A0B0C0D0E0F
Nonce = 000102030405060708090A0B0C0D0E0F
PT =
AD = 0000010102020303040405050606070780
CT = 00495ED7B0C4D7C68EEF975200245441

Key = 000102030405060708090A0B0C0D0E0F
Nonce = 000102030405060708090A0B0C0D0E0F
PT =
AD = 0000010102020303040405050606070700
CT = 00495ED7B0C4D7C68EEF975200245441
And with non empty PT:

Key = 000102030405060708090A0B0C0D0E0F
Nonce = 2A2B2C2D2E2F30313233343536373839
PT = 00
AD = 000001010203040504050606070780000000
CT = 5D45F0FC363C8C53A8A549D2A08A4BB455

Key = 000102030405060708090A0B0C0D0E0F
Nonce = 2A2B2C2D2E2F30313233343536373839
PT = 00
AD = 000001010203040504050606070780000000
CT = 5D45F0FC363C8C53A8A549D2A08A4BB455

And with Associated Data tails being 0x8080,0x0180, 0x0080

Key = 00000000000000000001010101010101
Nonce = 2A2B2C2D2E2F30313233343536373839
PT = 00
AD = 0000000000000000000000000000000180
CT = 7511E8F37303ADC8E7A352537D60342912

Key = 00000000000000000001010101010101
Nonce = 2A2B2C2D2E2F30313233343536373839
PT = 00
AD = 00000000000000000000000000000008080
CT = 7511E8F37303ADC8E7A352537D60342912
Key = 0000000000000000000000000000001010101010101
Nonce = 2A2B2C2D2E2F30313233343536373839
PT = 00
AD = 000000000000000000000000000000080
CT = 7511E8F37303ADC8E7A352537D60342912

This document, technology or software does not contain French national dual-use or military controlled data nor US national dual-use or military controlled data
Dear Alexandre and All,

Thanks to Alexandre for pointing out this issue. We would like to inform you that the collision that you have observed is due to an implementation error. The error was in line number 97 of the "encrypt.c" file of syconaer96128v1:

state[i]^=ad[num_ad_block*8+(u64)i];

The correct code needs 12 instead of 8. So this line should be replaced with

state[i]^=ad[num_ad_block*NUMRATEBYTES+(u64)i];

where NUMRATEBYTES is already defined as 12.

Please find the updated implementation as well as the change log attached, and note that our specification does not need any change due to this finding.

Thanks
Sycon Team

--
To unsubscribe from this group, send email to lwc-forum+unsubscribe@list.nist.gov
Visit this group at https://groups.google.com/a/list.nist.gov/d/forum/lwc-forum
Dear all,

It seems the latest version of SYCON (from June 6, 2019) is vulnerable to forgery attack.

This vulnerability comes from the use of identical domain separation tweaks for the last round of AD processing and the first rounds of PT processing.

This ruse of tweaks allows collisions between messages with empty and non-empty AD.

syconaer64128v1 and syconaer96128v1 are both vulnerable.

This vulnerability could be solved by changing one of the tweaks to guarantee separation between AD and PT processing.

Best regards,

Alexandre Mège

---

**Ex for syconaer96128v1**

- With empty AD

```
Key=0x000102030405060708090a0b0c0d0e0f
Nonce=0x2a2b2c2d2e2f30313233343536373839
Pt=0x
Ad=0x0000000000000000000101
Ct=0xa86826908bea8c24360bf5e53046fb95
```

```
Key=0x000102030405060708090a0b0c0d0e0f
Nonce=0x2a2b2c2d2e2f30313233343536373839
Pt=0x000000000000000000010101
Ad=0x
Ct=0xd2e652ca581478f431d684b1a86826908bea8c24360bf5e53046fb95
```
- With non empty AD

Key=0x000102030405060708090a0b0c0d0e0f
Nonce=0x2a2b2c2d2e2f30313233343536373839
Pt=0x00
Ad=0x0000000000
Ct=0x8cad6ea38e556440ee338091e78e4cc6

Key=0x000102030405060708090a0b0c0d0e0f
Nonce=0x2a2b2c2d2e2f30313233343536373839
Pt=0x00000000000100000000000000
Ad=0x
Ct=0xd2e652ca581578f431d785b08cad6ea38e556440ee338091e78e4cc6
Dear Alexandre and All,

Thanks to Alexandre for pointing out this issue. We would like to inform you that the collision that you have observed is due to an implementation error. The error was in the implementation of the domain separator. It is fixed now. As the test vectors provided in the specification are not affected by this fix, so they remain unchanged.

Please find the updated implementation as well as the change log attached.

We would like to inform you all that our specification does not need any change.

Thanks

Sycon Team

On Wed, Aug 14, 2019 at 12:18 PM MEGE, Alexandre <alexandre.mege@airbus.com> wrote:

Dear all,

It seems the latest version of SYCON (from June 6, 2019) is vulnerable to forgery attack.

This vulnerability comes from the use of identical domain separation tweaks for the last round of AD processing and the first rounds of PT processing.

This ruse of tweaks allows collisions between messages with empty and non-empty AD.

syconaer64128v1 and syconaer96128v1 are both vulnerable.

This vulnerability could be solved by changing one of the tweaks to guarantee separation between AD and PT processing.

Best regards,

Alexandre Mège

Ex for syconaer96128v1

- With empty AD
Dear all,
I confirm that the proposed fix solves the collision problem.
Thanks to the SYCON team for the quick update.
Best regards,
Alexandre Mège

---

From: Sumanta Sarkar [mailto:sumanta.sarkar@gmail.com]
Sent: Thursday, August 29, 2019 6:05 AM
To: MEGE, Alexandre
Cc: lightweight-crypto@nist.gov; lwc-forum@list.nist.gov
Subject: Re: [lwc-forum] OFFICIAL COMMENT: Sycon

Dear Alexandre and All,

Thanks to Alexandre for pointing out this issue. We would like to inform you that the collision that you have observed is due to an implementation error. The error was in the implementation of the domain separator. It is fixed now. As the test vectors provided in the specification are not affected by this fix, so they remain unchanged.

Please find the updated implementation as well as the change log attached.

We would like to inform you all that our specification does not need any change.

Thanks

Sycon Team

---

On Wed, Aug 14, 2019 at 12:18 PM MEGE, Alexandre <alexandre.mege@airbus.com> wrote:

Dear all,

It seems the latest version of SYCON (from June 6, 2019) is vulnerable to forgery attack.

This vulnerability comes from the use of identical domain separation tweaks for the last round of AD processing and the first rounds of PT processing.

This ruse of tweaks allows collisions between messages with empty and non-empty AD.

syconaer64128v1 and syconaer96128v1 are both vulnerable.

This vulnerability could be solved by changing one of the tweaks to guarantee separation between AD and PT processing.