

New issue

Jump to bottom

# Leaking control-flow (Frontal attack) #3394

Closed raoultrackx opened this issue on Jun 4, 2020 · 3 comments · Fixed by #3398

Assignees

Labels bug component-crypto

Projects Current sprint

Milestone June 2020 Sprint

raoultrackx commented on Jun 4, 2020 Contributor

Description

- Type: Bug
- Priority: Minor

Bug

**mbed TLS build:**  
Version: 2.16.6  
OS version: SGX

*Discoverers:* Ivan Puddu, Moritz Schneider, Miro Haller, Srdjan Capkun, ETH Zurich (i.e., not me)  
\*Short description: The authors describe in their paper a way to determine control flow in SGX enclaves by precisely timing interrupt latency. This succeeds even in balanced branches such as:

```
if (secret == 'a') {
    var1 = 1 + var1;
    var2 = 1 + var2;
} else {
    var1 = 2 + var1;
    var2 = 2 + var2;
}
```

The root cause of this is that the front-end of the processor fetches instructions with a 16 byte well-aligned window. The time to resume an instruction will depend on its location within this fetch window (and thus its virtual address) and instructions near it.  
*Full description:* <https://arxiv.org/abs/2005.11516>

*Solution:*

- Remove the secret dependent branch altogether

\*Code locations that require fixes:

- mpi\_montmul (bignum.c: 1924):

```
if( mbedtls_mpi_cmp_abs( A, N ) >= 0 )
    mpi_sub_hlp( n, N->p, A->p );
else
    /* prevent timing attacks */
    mpi_sub_hlp( n, A->p, T->p );
```

gilles-peskine-arm commented on Jun 4, 2020 Contributor

Thanks for letting us know! We do consider secret-dependent branches in private-key operations to be bugs when they are not protected by blinding, which this one isn't. We'll fix this one as soon as possible.

gilles-peskine-arm added bug component-crypto labels on Jun 4, 2020


raoultrackx commented on Jun 4, 2020 Contributor Author


Thanks!

gilles-peskine-arm self-assigned this on Jun 4, 2020


gilles-peskine-arm added this to To do in Current sprint via automation on Jun 4, 2020

gilles-peskine-arm moved this from To do to In progress in Current sprint on Jun 4, 2020

 gilles-pesquine-arm added this to the **June 2020 Sprint** milestone on Jun 4, 2020

 danh-arm added this to **In progress** in **Mbed TLS Current Sprint** on Jun 4, 2020

 gilles-pesquine-arm added a commit to gilles-pesquine-arm/mbedtls that referenced this issue on Jun 4, 2020

 Add changelog entry: `fix Mbed-TLS#3394` ...


58b5719

 gilles-pesquine-arm mentioned this issue on Jun 4, 2020


**Remove a secret-dependent branch in Montgomery multiplication #3398**

 Merged

 gilles-pesquine-arm added a commit to gilles-pesquine-arm/mbedtls that referenced this issue on Jun 4, 2020

 Add changelog entry: `fix Mbed-TLS#3394` ...

d55bfe9

 gilles-pesquine-arm added the `fix available` label on Jun 4, 2020

gilles-pesquine-arm commented on Jun 4, 2020

Contributor

It turns out that the leak was originally analyzed by [Sangho Lee](#), [Ming-Wei Shih](#), [Prasun Gera](#), [Taesoo Kim](#), and [Hyesoon Kim](#), Georgia Institute of Technology; [Marcus Peinado](#), Microsoft Research (cited in Puddu et al.). As far as I can tell, the Mbed TLS team was not aware of that 2017 paper until now.


 2

 raoultrackx mentioned this issue on Jun 9, 2020

**Mitigate Frontal attack** fortanix/rust-mbedtls#111


 Open

 gilles-pesquine-arm added a commit to gilles-pesquine-arm/mbedtls that referenced this issue on Jun 9, 2020

 Add changelog entry: `fix Mbed-TLS#3394` ...

5f56950

 gilles-pesquine-arm added a commit to gilles-pesquine-arm/mbedtls that referenced this issue on Jun 9, 2020

 Add changelog entry: `fix Mbed-TLS#3394` ...

70529ab

 yanesca closed this as completed in **#3398** on Jun 9, 2020


 **Mbed TLS Current Sprint**  moved this from **In progress** to **Done** on Jun 9, 2020

 daverodgman removed this from **Done** in **Mbed TLS Current Sprint** on Mar 30

#### Assignees

 gilles-pesquine-arm

#### Labels

 **component-crypto**

#### Projects

No open projects


1 closed project ▾

#### Milestone

June 2020 Sprint

#### Development

Successfully merging a pull request may close this issue.

 **Remove a secret-dependent branch in Montgomery multiplication**  
gilles-pesquine-arm/mbedtls

2 participants

