urandom

Computer Security Magazine

vol.11

Zenbleed脆弱性の解説 op

BLE通信を覗いてみよう S社編 mayth

目次

Zenbleed 脆弱性の解説

1 はじめに

2023 年 07 月 24 日、「Zenbleed」と名付けられた脆弱性[*1][*2]が公表された。この脆弱性は CPU のハードウェアに起因する情報漏洩の脆弱性で、AMD 社製の一部 CPU で動作するシステム上において、あるプロセスの一部レジスターを他のプロセスから読み取れるというものである。脆弱性の詳細は基本的に発見者の Tavis Ormandy 氏が公開した記事[*3]の通りだが、この記事では発見者記事や関連するドキュメントを元に筆者による補足などを交えつつ解説を行う。なお、発見者と筆者に関係は無く、この記事は筆者の理解の範囲で解説を行うものであって、文責は筆者にある。

2 前提条件と制約

この脆弱性を利用すると、一定のパターンに沿う命令列を Zen 2 アーキテクチャーの CPU 上で実行した時、ある程度の確率で他プロセスの YMM レジスターの一部を読み取れる。読み取り先のプロセスは読み取り元のプロセスと同一の物理コアで動作している必要がある。CPU のハードウェアに起因する事象なので、使用している OS、プロセスの権限レベルや VM のゲスト・ホストといった要素は基本的に関係無い。

つまり、脆弱性を利用され得るのは、次の全条件が成立した場合となる。

- 対象のシステムが Zen 2 アーキテクチャーの CPU で動作していること
- システム上で任意の命令列を実行できること
  - 権限レベルや VM の内外などは問わない
- 読み取り先のプロセスが読み取り元のプロセスと同一物理コアで動作していること
- 後述する緩和策が施されていないこと

[*1] CVE-2023-20593

[*2] AMD, Cross-Process Information Leak `https://www.amd.com/en/resources/product-security/bulletin/amd-sb-7008.html`

[*3] Tavis Ormandy, Zenbleed `https://lock.cmpxchg8b.com/zenbleed.html`

手元での実験で読み取れたのは各 YMM レジスターの上位 128bit のみだった。この結果は後述の示唆されるメカニズムと矛盾しないので、これがこの脆弱性の制約である可能性があるが、筆者が知る限りで AMD 社や発見者は明言しておらず、他環境では異なる可能性は否定できない。読み取るレジスターの選択はあまり制御が効かず[*4]都度違うレジスターが読み取れるものの、十分高い確率で読み取れるので、繰り返し読み取りを行うことで全ての YMM レジスターが読み取られ得る。

3 調査環境

記事中で使用した実験環境は次の通り。

CPU
: AMD Ryzen 5 3600 6-Core Processor

Microcode
: 0x8701021 [*5]

RAM
: 16GB

OS
: Ubuntu 22.04.2 LTS

Linux
: 6.2.0-26-generic, #26~22.04.1-Ubuntu SMP PREEMPT_DYNAMIC Thu Jul 13 16:27:29 UTC 2

PoC
: `https://github.com/google/security-research/tree/master/pocs/cpus/zenbleed` (commit 4706ef7048caeafc1035adf296d011d1b4941b2f)

今回使用した Ryzen 5 3600 は 6 コア 12 スレッドの CPU で、トポロジー上は $n = 0 - 5$ について論理コア番号 n と $n + 6$ が同時マルチスレッディング（SMT）により同一の物理コア n 上で動作する[*6]。

[*4] 実行する命令列の調整である程度の傾向は持たせられる。`https://github.com/google/security-research/blob/4706ef7048caeafc1035adf296d011d1b4941b2f/pocs/cpus/zenbleed/zenleak.asm#L99` を参照。

[*5] 公開日は不明だが Google 検索の情報から 2020 年頃のものと推測する。

[*6] 論理コア 0 と 6 が物理コア 0、論理コア 1 と 7 が物理コア 1.....論理コア 5 と 11 が物理コア 5 で動作する。

BLE の通信を覗いてみよう - S 社編

1 注意

本稿では無線通信の傍受を取り扱いますが、すべて自身が所有・管理するデバイス同士が行う通信に対して、実験として傍受を行っています。本稿の内容を実際に試す際には、必ず自己の管理下において実施するようお願いします。他者の通信を傍受し、その存在を明かすこと、またはその内容を利用することは犯罪となる恐れがあります。

2 はじめに

C99A（2021 年冬コミ）にて頒布した “urandom vol.8”[*1]で BLE の通信を傍受する記事を書きましたが、このときは通信の傍受と通信内容の簡単な分析まで行いました。また、適当なクライアントを用意して通信を再現し、専用のアプリなしでもデバイスを制御することを目指しましたが、通信が上手くいかず断念しました。

今回はそのリベンジということで、前回と同様にカーテンを操作するデバイスをターゲットとして傍受と通信内容の分析を試みます。

なお、BLE とはそもそもなんぞやとか、この記事のモチベーションなんかは前回の記事を参照頂ければと思います。

3 ハードウェアの準備

3.1 使用機材

通常の BLE 対応デバイスでは BLE の通信を傍受することはできません。今回は Adafruit の “Feather nRF52840 Express” を使用しました。秋月電子通商[*2]やスイッチサイエンス[*3]で入手できます。前回使用した “Bluefruit LE Sniffer” と異なり、これはそのままスニッ

[*1] https://urandom.team/books/urandom-vol8/（電子版は執筆時現在未発刊）
[*2] https://akizukidenshi.com/catalog/g/gM-16358/ 執筆時 3,080 円
[*3] https://www.switch-science.com/products/5400 執筆時 4,697 円

ファーとして使えるデバイスではありません。ファームウェアを書き換えることでスニッファーとして使えるようになります。

傍受の対象となるデバイスは前回同様にカーテンを自動で開閉するデバイスです。ただし、前回とは異なるメーカーの製品を使用しています。機能的には概ね同じで、タイマーの設定や開閉制御は専用のアプリをスマートフォンにインストールして行います。また、Wi-Fi に接続されたハブとなるデバイスがあれば外出先からの制御も可能です。

専用のアプリは中古で入手した Pixel 3 にインストールしました。

最後に、今回使用したマシンの詳細は以下の通りです。

機種	Apple MacBook Pro（14 インチ, 2021）
CPU	Apple M1 Max (ARM64)
OS	macOS Ventura (13.4)

3.2 Feather nRF52840 Express のブートローダー更新

今回は UF2 によるファームウェア書き込みを行いたいのですが、それにはブートローダーのバージョンが 0.4.0 以降でなくてはなりません。そこでまず入手した Feather nRF52840 Express のブートローダーのバージョンを確認します。ホストマシンと接続した状態でボード上にあるリセットスイッチを素早く 2 回押すと、ホストから ***BOOT という名前のリムーバブルディスクとして認識されます。今回は FTHR840BOOT として認識されていました。この中にある INFO_UF2.TXT にブートローダーのバージョンが記載されています。

```
› cat /Volumes/FTHR840BOOT/INFO_UF2.TXT
UF2 Bootloader 0.2.6 lib/nrfx (v1.1.0-1-g096e770) lib/tinyusb (legacy-525-ga1c59649)
      s140 6.1.1
Model: Adafruit Feather nRF52840 Express
Board-ID: NRF52-Bluefruit-v0
Bootloader: s140 6.1.1
Date: Dec 21 2018
```

バージョン 0.2.6 とのことなので、まずコマンドラインからブートローダーを更新します。もし 0.4.0 以降のブートローダーが最初から入っていればこの手順は飛ばします。

“Adafruit nRF52 Bootloader” の Release[*4]から最新のものを選び、さらにそこから feather_nrf52840_express_bootloader-*.zip を探してダウンロードします（* にはバージョン等が入ります）。今回は 0.7.0 をダウンロードしました。

ブートローダーの書き込みに必要なツールである adafruit-nrfutil をインストールします。

```
› pip3 install adafruit-nrfutil
```

[*4] https://github.com/adafruit/Adafruit_nRF52_Bootloader/releases/

urandom vol.11

発行者	urandom
表紙デザイン	秋弦めい
発行日	2023 年 8 月 13 日
バージョン	1.00
コミット ID	ab44df6
連絡先	https://urandom.team/
印刷所	株式会社ポプルス

urandom

presented by urandom

Comic Market 102 (Aug. 13th, 2023)