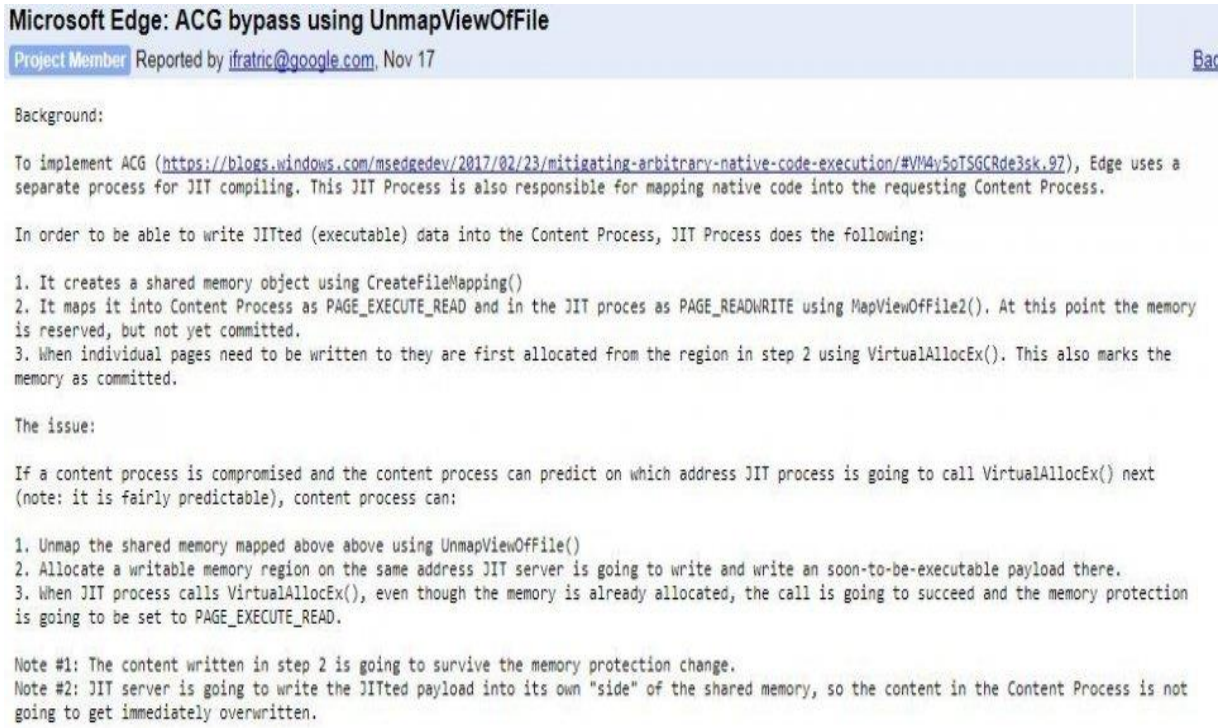
Google 又在微軟修補前公佈 Microsoft Edge 漏洞

Google Project Zero 安全團隊去年 11 月發現一可繞過 Microsoft Edge ACG 漏洞，讓攻擊者透過 Microsoft Edge 將未獲簽章的惡意程式碼載入 Windows 電腦。儘管已通報微軟，但微軟尚未完成修補，本周末以超出期限為由公佈漏洞資訊。

文/林妍溱 | 2018-02-20 發表



Microsoft Edge: ACG bypass using UnmapViewOfFile

Project Member Reported by ifratric@google.com, Nov 17

Background:

To implement ACG (https://blogs.windows.com/msedgedev/2017/02/23/mitigating-arbitrary-native-code-execution/#VM4y5qTSGCRde3sk.97), Edge uses a separate process for JIT compiling. This JIT Process is also responsible for mapping native code into the requesting Content Process.

In order to be able to write JITted (executable) data into the Content Process, JIT Process does the following:

1. It creates a shared memory object using CreateFileMapping()
2. It maps it into Content Process as PAGE_EXECUTE_READ and in the JIT proces as PAGE_READWRITE using MapViewOfFile2(). At this point the memory is reserved, but not yet committed.
3. When individual pages need to be written to they are first allocated from the region in step 2 using VirtualAllocEx(). This also marks the memory as committed.

The issue:

If a content process is compromised and the content process can predict on which address JIT process is going to call VirtualAllocEx() next (note: it is fairly predictable), content process can:

1. Unmap the shared memory mapped above above using UnmapViewOfFile()
2. Allocate a writable memory region on the same address JIT server is going to write and write an soon-to-be-executable payload there.
3. When JIT process calls VirtualAllocEx(), even though the memory is already allocated, the call is going to succeed and the memory protection is going to be set to PAGE_EXECUTE_READ.

Note #1: The content written in step 2 is going to survive the memory protection change.
Note #2: JIT server is going to write the JITted payload into its own "side" of the shared memory, so the content in the Content Process is not going to get immediately overwritten.

Google Project Zero 本周末又以超出期限為由公佈微軟尚未修補完成 Microsoft Edge 中一個可能導致惡意網頁下載到 Windows PC 的安全功能漏洞。

這項漏洞位於 Microsoft Edge 中的任意程式碼防護（Arbitrary Code Guard, ACG），它是微軟於 2017 年 4 月的 Windows 10 Creators Update 加入 Microsoft Edge 瀏覽器的兩項安全功能之一：ACG 結合另一項功能 Code Integrity Guard（CIG）可防止 JavaScript 將惡意程式碼透過瀏覽器載入 Windows 記憶體執行，唯有獲得簽章的網頁才能執行。

Google Project 安全研究員 Ivan Fratric 去年 11 月發現一項可繞過 ACG 的漏洞，可讓攻擊者透過 Microsoft Edge 將未獲簽章的惡意程式碼載入 Windows 電腦。他隨後將此漏洞通報微軟。

按照 Project Zero 的慣例，漏洞通報後軟體業者有 90 天可以修補。本月 15 日微軟回覆修補工作複雜度超出預期，微軟可能無法在 2 月安全更新這個記憶體管理問題，但有信心可以在 3 月 13 日完成。

不過 Fratric 以已經超過 90 天修補期，以及配合微軟周二更新而多寬限的 14 天期間為由，公佈了這項漏洞。

這已是 Google 近年自 2015 年及 2017 年初後，第三次在微軟修補完成產品漏洞前公諸於世。前兩次都引發微軟對 Google 的批評，並

曾經於去年 10 月以牙還牙，公佈 Google Chrome 的漏洞，還藉此拿到 Google 抓漏獎金。

資料來源：iThome