مجلة السلفيوم للعلوم والتقنية

SILPHIUM JOURNAL OF SCIENCE AND TECHNOLOGY

(SJST)

مجلة علمية محكمة تصدر عن

المعهد العالي للعلوم والتقنية شحات

Higher Institute of Science and Technology - Cyrene

العدد الثالث يناير 2023م

SJST Vol.03 No 01 2023

مجلة السلفيوم للعلوم والتقنية

مجلة علمية محكمة نصف سنوية تصدر عن المعهد العالي للعلوم والتقنية شحات

رقم الإيداع القانوني بدار الكتب الوطنية

2023/619

العنوان: المعهد العالي للعلوم والتقنية شحات ليبيا

الموقع الالكتروني:

www.j.istc.edu.ly

البريد الالكتروني:

sjst@istc.edu.ly

رقم الهاتف:

0914274759

العدد الثالث

يناير 2023م

SJST Vol.03 No 01 2023

الشروط العامة لضمان الموافقة على النشر:

- الاهتمام بأصالة المحتوى.
- التأكد من عدم نشر البحث في أي مجلة أخرى.
- التأكد من اتباع أخلاقيات البحث في الإعداد.

هـيـئـة تـحـريـر الـمـجـلـــة

محتويات العدد

كلمة رئيس التحرير

افتتاحية العدد الثالث

بسم اللّه الرحمن الرحيم

الحمد للّه رب العالمين، والصلاة والسلام على أشرف المرسلين، سيد الخلق سيدنا محمد وعلى آله وصحبه والتابعين.وبعد:

فهذا العدد الثالث من مجلة السلفيوم للعلوم والتقنية يصدر باسم المعهد العالي للعلوم والتقنية ببلدية شحات تحت رعاية وزارة التعليم التقني ، والتي أخذت على عاتقها دعم هذه المجلة، ليستمر عطاؤها وتواصلها في فتح آفاق للمعرفة والبحث العلمي، في تخصصاتها المتنوعة.

يأتي هذا العدد وقد حوى بحوثا قيّمة في علوم شتى، نسأل اللّه تعالى أن يهدي بها وينفع، ويدفع الباحثين إلى مزيد من البحوث، هي زاد قادم الأعداد بإذنه تعالى وكرمه.

وفي الختام فإن هيئة التحرير تتقدم بشكرها وامتنانها لكل أصحاب الأيادي من البحاث والمقيمين والإداريين والمحبين، واللّه نسأل أن يجعل جهودهم وما قدموا ويقدمون في موازين حسناتهم .

واللّه ولي التوفيق

والسّلام عليكم ورحمة اللّه وبركاته

رئاسة تحرير المجلة

عنهم: د.منصور سالم عبدالرواف

رئيس التحرير

أهداف المجلة

- تختص المجلة بنشر نتائج الأبحاث والدراسات والمقالات التي يقوم بها أو يشترك في إجرائها أعضاء هيئات التدريس والباحثون في الجامعات والمعاهد العلمية ومراكز البحوث وهيئات البحث العلمي في مجالات العلوم التكنولوجيا (والعلوم المرتبطة بها).
- التطوير المستمر في أساليب النشر والتحكيم والتبادل العلمي مع الجهات المحلية والخارجية
- المساهمة في رفع ترتيب المعهد العالي للعلوم والتقنية شحات بين الجامعات والمعاهد العليا في ليبيا.
- المنافسة مع المجلات العالمية المتخصصة واحتلال مكانة رفيعة بينها.

رسالة المجلة

- نشر الأبحاث العلمية وفق معايير منضبطة بما يحافظ على الأصالة، والمنهجية، والقيم العلمية، ويدعم الإبداع الفكري.
- التميز في تقديم البحوث ذات الأفكار المبتكرة والتي لم يسبق نشرها بمجلات علمية أخرى والمحكمة بواسطة نخبة من العلماء والمتخصصين والإسهام في إخراج بحوث علمية متميزة، وتتحقق رسالتنا من خلال الالتزام بالمعايير العالمية للتميزفي مجالات البحث العلمي.

رؤية المجلة

- الريادة العالمية والتميز في نشر البحوث الرائدة المبتكرة الأصيلة؛ لتكون خيار الباحثين الأول لنشر بحوثهم العلمية .
- توثيق ونشر الثقافة العلمية بين الباحثين والتواصل العلمي في مختلف مجالات العلوم التقنية.
- تشجيع قنوات الاتصال بين المختصين في شتي مجالات العلوم والمؤسسات الإنتاجية والتعليمية.
- الارتقاء بمستوى العلوم والأبحاث التطبيقية لخدمة المؤسسات الإنتاجية بليبيا وتطويرها باستحداث الأساليب والوسائل المستخدمة من خلال إصدارات المجلة.

قواعد النشر بالمجلة

- يتم تقديم البحوث المعدة وفقا لشروط المجلة بإرسالها الى البريد الإلكتروني الخاص بالمجلة التالي:
((SJST@ISTC.EDU.LY)) (نسخة الكترونية واحدة ملف Word).
- تقبل المجلة البحوث العلمية الأصيلة ذات الأفكار المبتكرة والتي لم يسبق نشرها بمجلات أخرى او مؤتمرات وذلك للنشر باللغة الا نجليزية مع ملخص باللغة العربية أو باللغة العربية مع ملخص باللغة الا نجليزية.
- يمكن تقديم البحوث للنشر بالمجلة بعد إعدادها حسب قواعد كتابة البحث الخاصة بالمجلة.
- تنشر البحوث في المجلة حسب أسبقية ورودها وقبول المحكمين للبحث وإعدادها من قبل الباحثين ومراجعتها من قبل هيئة التحرير في أول عدد يصدر عقب انتهاء هذه الإجراءات.
- يرسل البحث بعد استلامه الى اثنين من المحكمين في ذات التخصص وتستعجل تقارير المحكمين بعد شهر من تاريخ إرسال البحث الى المحكم ويسند تحكيم البحث الى محكم أخر عند تأخر التقرير عن شهرين.
- يرفض نشر البحث إذا رفض المحكمين البحث أما إذا كان الرفض من محكم واحد فيرسل البحث لمحكم ثالث ويكون رأيه هو الفيصل.
- بعد قيام الباحث بإجراء التعديلات المطلوبة من قبل المحكمين يرسل البحث الى أحد أعضاء هيئة التحرير للمطابقة.
- يعرض البحث في صورته النهائية علي الباحث (الباحثين) قبل وضعه Online في موقع المجلة.
- يتم طلب دفع رسوم التحكيم من قبل الباحث وطلب صورة عملية التحويل بإرسالها الى البريد الإلكتروني الخاص بالمجلة.
- يتم إبلاغ الباحث ببريد الكتروني رسمي بإتمام عملية النشرفي حال إكمال كافة الإجراءات السابقة وإنجاز عملية النشر الفعلي في عدد المجلة و يحصل الباحث على نسخة إلكترونية من العدد الذي اشتمل على البحث المطلوب نشره.
- يجب أن يشتمل البحث على الأقسام الآتية: العنوان ، المؤلف(المؤلفون) ، الكلمات المفتاحية، الملخص (بلغة البحث) ، المقدمة ، طرق البحث ، النتائج و المناقشة و التوصيات، المراجع (يجب فصل النتائج عن المناقشة) ، وأخيرا ملخص باللغة العربية أو الإنجليزية (ليست اللغة المستخدمة لمتن البحث) و يستعمل برنامج Microsoft Office على ورق مقاس A4.

مواصفات تنسيق البحوث:

- يتم استخدام خط Times new Roman حجم 12 لمحتوى البحث واستخدام مسافة 1.25 بين أسطر النصوص، ويتم اعتماد خط 12 غامق اللون (Bold) للعناوين الرئيسية ، و10 لعناوين الجداول والرسومات، ويتم استخدام حجم خط 14 لعنوان الدراسة في الصفحة الرئيسية و12 لأسماء الباحثين علي أن تضبط الهوامش على مسافة 2.5 سم من جميع الاتجاهات.
- يتم كتابة أسماء الباحثين بالترتيب الطبيعي (الاسم الأول ثم الأب ثم اللقب) لكل منهم شاملة جهات عملهم و يحدد اسم الباحث المسئول (Corresponding Author) عن المراسلات بعلامة* ويذكر العنوان الذى يمكن مراسلته عليه وعنوان البريد الالكتروني.
- يجب أن لا يزيد عدد صفحات البحث عن 25صفحة وفي حال زيادة عدد الصفحات عن المذكور فسيتم إضافة رسوم وفقا لحجم الزيادة مقارنة بعدد الصفحات المحددة في المجلة.
- يجب إرفاق ملخص مكون من 250-300 كلمة باللغتين العربية والإنجليزية، بالإضافة إلى ضرورة توفير ما لايقل عن 4 كلمات مفتاحية لمحتوى الملخص العربي والإنجليزي.

البحوث التي احتواها العدد الثالث

اولا: البحوث العربية:

ثانيا: البحوث الانجليزية

A Study to analysis the effect of the vulnerability CVE 2016 7256 in several Versions of windows and the strategies used to decrease its vulnerability

OSAMA FARAJ MOHAMED

Department of computer, Faculty of Education, Omar Al-Muktar University, Albyda, Libya

ASHRAF MOHAMED ABDALLA

Department of computer, Faculty of Education, Omar Al-Muktar University, Albyda, Libya

Osama.mohamed@omu.edu.ly

Mohamed, Abdalla / SILPHIUM Journal of Science and Technology. 3(1), 2023, 61-75.

Research Article

SILPHIUM JOURNAL OF SCIENCE AND TECHNOLOGY

(SJST)

A Study to analysis the effect of the vulnerability CVE 2016 7256 in several Versions of windows and the strategies used to decrease its vulnerability

Osama Faraj Mohamed[1*], Ashraf Mohamed Abdalla[1]

[1] *Department of computer, Faculty of Education, Omar Al-Muktar University, Albyda, Libya*

**Corresponding Email:* Osama.mohamed@omu.edu.ly

Received 22/09/2022 Revised 04/12/2022 Published online 18/01/2023

ABSTRACT

Vulnerability verification and exploitation are evolving into an essential part of security, particularly in distributing malware code, system hacking, efforts to generate patches, improving the source code, or software updates. Vulnerabilities in media, programs, including browsers, readers of documents, players, and internet services.

This paper discusses user-level through system administrator-level mitigation strategies for the CVE-2016-7256 vulnerabilities. Windows is used to evaluate the two different files; one file is patched, and the second one is not acquired from a new installation to understand the module's technological component and how this affects the operational mechanism. We will be able to identify the modules that cause system vulnerabilities due to this. With WinDBG, a stack trace may be performed to identify the appliance call from when it was received to when the exemption was triggered. However, this stack trace can easily be performed if the system can crash. As a result, the crash can be investigated in the stack, and the heap since memory is dynamically assigned to them. Additionally, this paper will illustrate how the system may be kept secure by managing the server well.

Keywords: *Attack, vulnerability, Windows security, CVE-2016-7256, Threat*

دراسة لتحليل تأثير الثغرة الأمنية CVE 2016 7256 في عدة إصدارات لنظام التشغيل ويندوز والاستراتيجيات المستخدمة لتقليل الثغرات لها

أسامة فرج هويدي محمد[1]*، أشرف محمد المبروك[1]

[1] قسم الحاسوب، كلية التربية، جامعة عمر المختار، البيضاء، ليبيا

***للمراسلة: Osama.mohamed@omu.edu.ly**

الملخص

اليوم زادت تهديدات الكمبيوتر من المهاجمين أكثر من أي وقت مضى و يستغل المهاجمون إمكانات الهندسة الاجتماعية لإنشاء برامج ضارة وإرسالها في شكل رسائل البريد الإلكتروني ورسائل الوسائط الاجتماعية إلى شبكات الكمبيوتر العامة والمؤسسة بمجرد حدوث مثل هذه الهجمات ، يلاحظ (Symantec 2015) أن التخفيف يصبح صعبًا خاصة بسبب نقص المعرفة العامة.

تم توجيه الهجمات ضد كل من المنظمات والأشخاص مما أدى إلى فقدان المعلومات الحساسة بما في ذلك تفاصيل البنوك وكلمات المرور. ومع ذلك ، هناك مشكلات حرجة حيث لا يحتاج المهاجمون إلى إذن من المستخدم لاستكشاف حساباتهم وقد يؤدي ذلك إلى فقدان الكثير من المعلومات (Symantec 2015b؛ Moran، 2012؛ Joh and Malaiya، 2010؛ Davis ،Bodmer and Lemasters ،2010).

أخيرًا ، تتم في هذه الورقة مناقشة طرق التخفيف من الثغرات الأمنية التي تطرحها CVE-2016-7256 مباشرة من مستوى المستخدم إلى مسؤول النظام. علاوة على ذلك ، سيتم شرح أمان النظام من خلال أفضل إدارة للخادم في هذه الورقة.

الكلمات المفتاحية: الهجوم، الثغرة ، أمن الويندوز، نقاط الضعف ، الثغرة الامنية 2016-7256

INTRODUCTION

The ability to quickly defeat the security threat in software systems has improved thanks to vulnerability identification and patch file production. Patch files allow for the possibility of an automatic exploit. Patches for insecure code are crucial for ensuring security precautions. Previous studies have shown that anytime a patch is released, an attacker (Hacker) may quickly utilize it to pinpoint the precise location of the problematic code and immediately produce an exploit. It is different from what you are used to. The approach is remarkably adaptable while developing software. According to Akram, J., and Luo, P.(2020), it is reasonably challenging to distinguish between source code and cloned source code. This paper discusses CVE-2016-7256 vulnerability by looking at its technical and functional details. The discussion includes the Windows Operating System affected by the vulnerability and the damages that could follow. The threat posed by CVE-2016-7256 is also discussed, in addition to how attackers exploit the vulnerability and how it works. Recommendations for the mitigation of this vulnerability are also provided in this paper.

1. The vulnerability CVE-2016-7256 According to the National Vulnerability Database (NVD) (2016), vulnerability CVE-2016-7256 has an effect on the atmfd.dll in the Windows font library in the following operating systems;

- Microsoft Windows Vista SP2
- Windows 7 SP1
- Windows Server 2008 SP2 and R2 SP1
- Windows 8.1
- Windows RT 8.1
- Windows Server 2012 Gold and R2

- Windows 10 Gold, 1511, and 1607
- Windows Server 2016

The CVE-2016-7256 vulnerability paves the way for attackers to execute arbitrary code through a crafted website in what is technically called Open Type Font Remote Code Execution Vulnerability. Such an attack facilitates the hacker to perform a series of activities on the user system, including removing data, running programs, making system changes, and adding users with high privileges. However, the harm is usually less if a system with minimum user rights is exploited. Due to the effect of the attack caused by this vulnerability, CVE-2016-7256 is nowadays considered one of the worst weaknesses in a computer system. As shown in Figure follows.

#	CVE ID	CWE ID	Vulnerability Type(s)	Publish Date	Update Date	Score	Gained Access Level	Access	Complexity	Authentication	Conf.	Integ.	Avail.
1	CVE-2016-7256	284	Exec Code	2016-11-10	2016-11-28	9.3	None	Remote	Medium	Not required	Complete	Complete	Complete

atmfd.dll in the Windows font library in Microsoft Windows Vista SP2, Windows Server 2008 SP2 and R2 SP1, Windows 7 SP1, Windows 8.1, Windows Server 2012 Gold and R2, Windows RT 8.1, Windows 10 Gold, 1511, and 1607, and Windows Server 2016 allows remote attackers to execute arbitrary code via a crafted web site, aka "Open Type Font Remote Code Execution Vulnerability."

2	CVE-2016-7255	264	+Priv	2016-11-10	2016-11-28	7.2	None	Local	Low	Not required	Complete	Complete	Complete

The kernel-mode drivers in Microsoft Windows Vista SP2, Windows Server 2008 SP2 and R2 SP1, Windows 7 SP1, Windows 8.1, Windows Server 2012 Gold and R2, Windows RT 8.1, Windows 10 Gold, 1511, and 1607, and Windows Server 2016 allow local users to gain privileges via a crafted application, aka "Win32k Elevation of Privilege Vulnerability."

3	CVE-2016-7248	284	Exec Code	2016-11-10	2016-11-28	9.3	None	Remote	Medium	Not required	Complete	Complete	Complete

Microsoft Video Control in Microsoft Windows Vista SP2, Windows 7 SP1, Windows 8.1, Windows RT 8.1, and Windows 10 Gold, 1511, and 1607 allows remote attackers to execute arbitrary code via a crafted file, aka "Microsoft Video Control Remote Code Execution Vulnerability."

4	CVE-2016-7247	284	Bypass	2016-11-10	2016-12-02	5.0	None	Remote	Low	Not required	None	Partial	None

Microsoft Windows 8.1, Windows Server 2012 Gold and R2, Windows RT 8.1, Windows 10 Gold, 1511, and 1607, and Windows Server 2016 allow physically proximate attackers to bypass the Secure Boot protection mechanism via a crafted boot policy, aka "Secure Boot Component Vulnerability."

5	CVE-2016-7246	264	+Priv	2016-11-10	2016-11-28	7.2	None	Local	Low	Not required	Complete	Complete	Complete

The kernel-mode drivers in Microsoft Windows Server 2008 R2 SP1, Windows 7 SP1, Windows 8.1, Windows Server 2012 Gold and R2, Windows RT 8.1, Windows 10 Gold, 1511, and 1607, and Windows Server 2016 allow local users to gain privileges via a crafted application, aka "Win32k Elevation of Privilege Vulnerability."

Figur1: Order of vulnerability cve 7256

What is atmfd.dll?

Atmfd.dll is an Adobe Manager developed by Adobe Systems Incorporated Animesh Jain, V.S.P.M. (2022). It is developed based on its version. Some of the information of atmfd.dll include;

- Microsoft Windows digitally signs it.
- In Windows, it is described as Windows NT OpenType/Type 1 Font Driver.
- Its path of location is: 'c:\Windows\SoftwareDistribution\Download\aae4de72bcf4ba076c52dd35e348b10b\amd64_microsoft-windows-gdi_31bf3856ad364e35_6.1.7601.18768_none_07c6fc77714aec8d\' folder.
- Scanning it using the anti-virus scanners does not report atmfd.dll as malicious.

A Microsoft security bulletin MS16-132 provides an update for the security of the Microsoft Graphics component and resolves the vulnerabilities of Microsoft OS, including the execution of a remote code. According to Microsoft (2016), this vulnerability comes from the improper handling of specially crafted and embedded fonts by the Windows font

library. The bulletin MS16-132, therefore, addresses the following vulnerabilities;

- Open Type Font Information Disclosure Vulnerability.
- Open Type Font Elevation of Privilege Vulnerability.
- Windows Animation Manager Memory Corruption Vulnerability.
- Media Foundation Memory Corruption Vulnerability.

Remote Code Execution (RCE) refers to a situation where the attacker succeeds in penetrating a network remotely. RCE is the most common type of exploit in Windows OS. For example, an attacker can exploit a browser vulnerability to run or download malicious codes or programs. Such kind of an attack is known as a drive-by download.
Another attack is known as Local Privilege Escalation (LPE). In LPE, the attacker tries to acquire the highest privileges and is done when the system has already been exploited or compromised. Baranov (2016) notes that exploited LPE vulnerabilities are usually located in the standard Windows win32k.sys driver, making it easy for the attacker to get the full privileges of the system and even run malicious codes in kernel mode (Ring 0) once he succeeds in exploiting the vulnerability in win32k.sys.
The objective of this study:

According to Kaspersky (2015), this is a severe vulnerability and can be exploited by hackers to interrupt the client's services, bypass security restrictions, obtain privileges or get valuable information recently discovered in Microsoft Windows. Understanding this vulnerability is critical to successful technical analysis using the right debugging tools

Methodology

Analyzing the patched and un-patched atmfd.dll:

According to (Tang. J. 2016), the vulnerability that influences the atmfd.dll is extremely simple. This occurred while appliance calls accumulated on the GDI API; hence it may select the font drivers to access throughout the font processing. As a result, the ATMFD.DLL occurs to be one of these font drivers. Therefore, while the ATMFD.DLL module processes the font information, a buffer underflow is formed by a signed enlarging. According to Domars (2022), to comprehend the module's technological component and how this influences the operating mechanism, windows are employed to examine the two diverse files; one file is patched, and the second is not obtained from a new install. This will allow us to distinguish the modules leading to system vulnerabilities. A stack trace can be conducted through WinDBG to recognize the appliance call once processed to the moment the exemption was activated. Nevertheless, this stack trace can be carried out if the system can be crashed. Therefore, given that memory is assigned dynamically in the stack and the heap, the crash can be examined within the two positions.

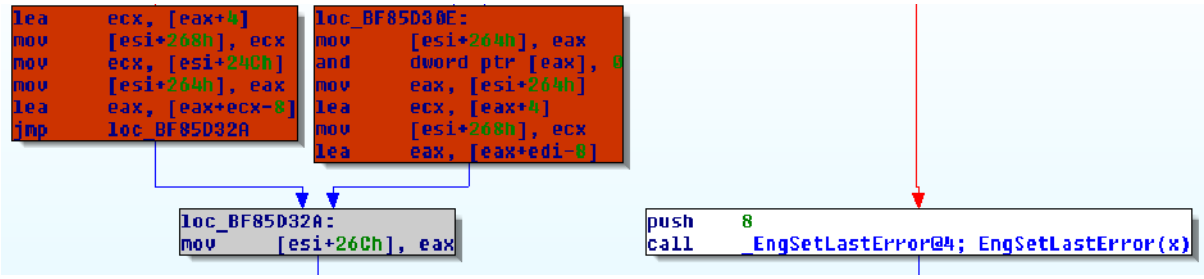
RESULTS

Differences &Results:

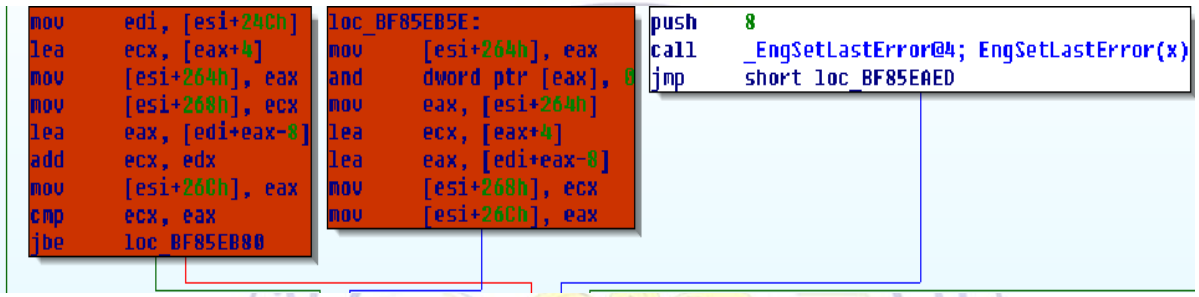
To examine the drives, ATMFD.DLL prior to and after is being patched. Ida Pro is applied and integrated, as well as a plug-in known as patch diff. This permitted us to show the dissimilarity before and after the scheme was patched, as shown in the subsequent IDA pro representations that show evident dissimilarity between the two files. The initial file on the un-patched files begins driving and calling roles on the subsequent line. In contrast, the

patched folder is driving and calling roles and also incorporated a Jump instruction shown on the following line.

2.1.1. Un-patched files:



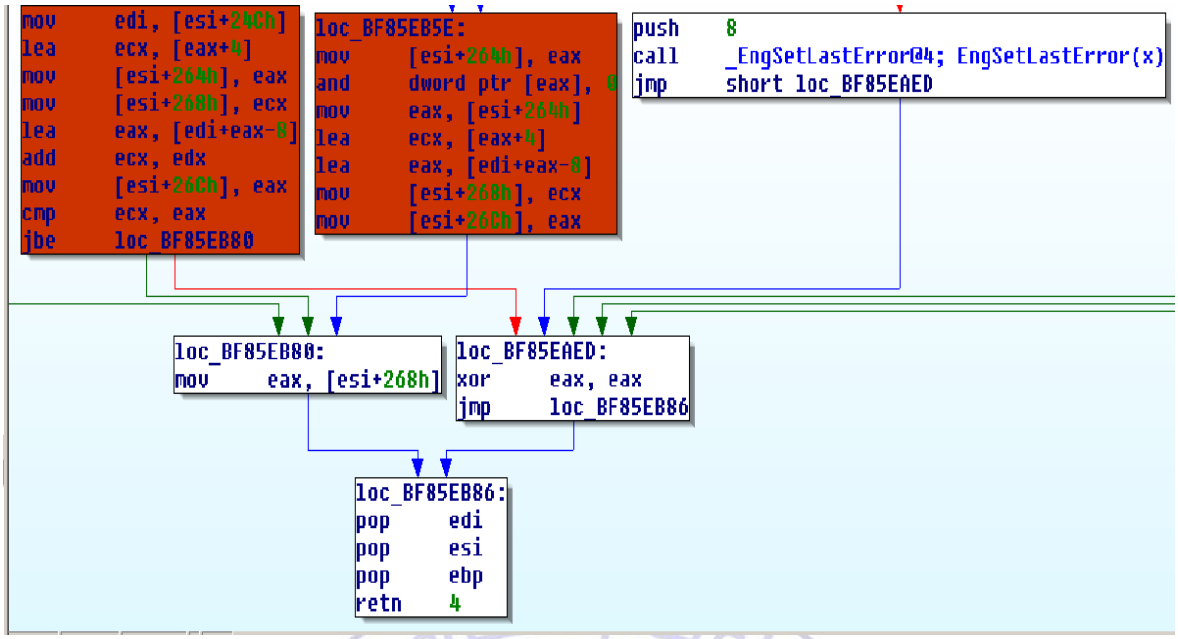
Patched file



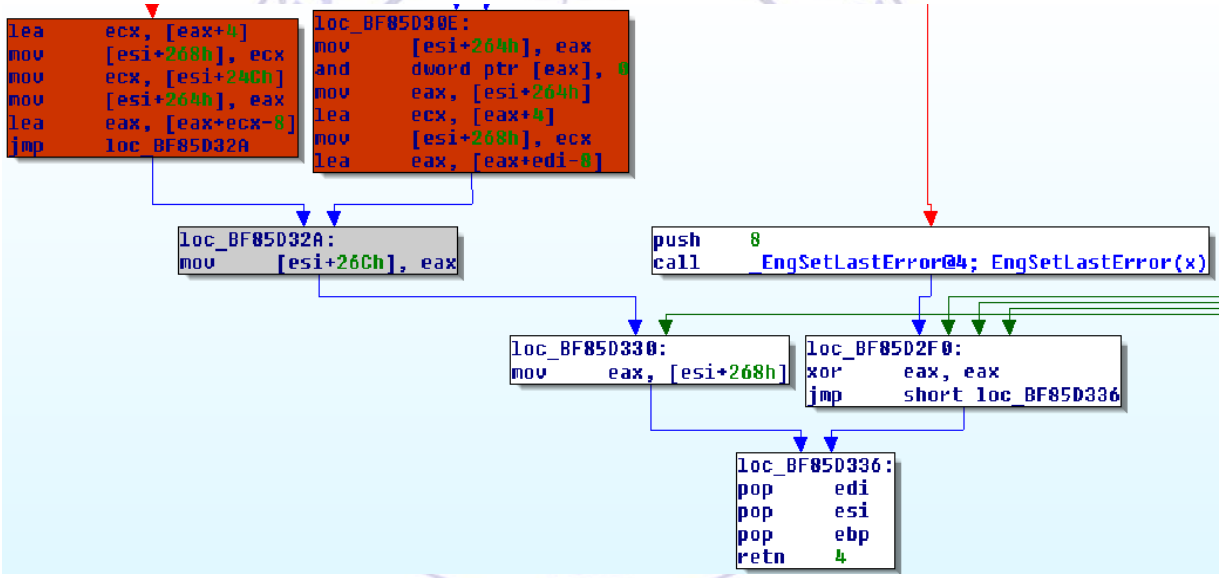
2.1.2 Patched file:

IDA pro could demonstrate similar roles and Un-Identical roles between the two folders, for instance, RFONTOBJ pgbCheckGlyphCache &RFONTOBJpgbBtextExt. The following files show the patched files and the un-patched files. Considering the disparities within the files, we realize that, within the un-patched files, the means of instructing LEA ECX [RAX+4] is by including 4 bytes to the EAX hence loading them to the ECX list. Conversely, about the patched files, we realize that the means of instructing MOV EDI [ESI+24CH] is by adding 24 bytes into the EDI list. This is the third line on the block demonstrated within the subsequent images.

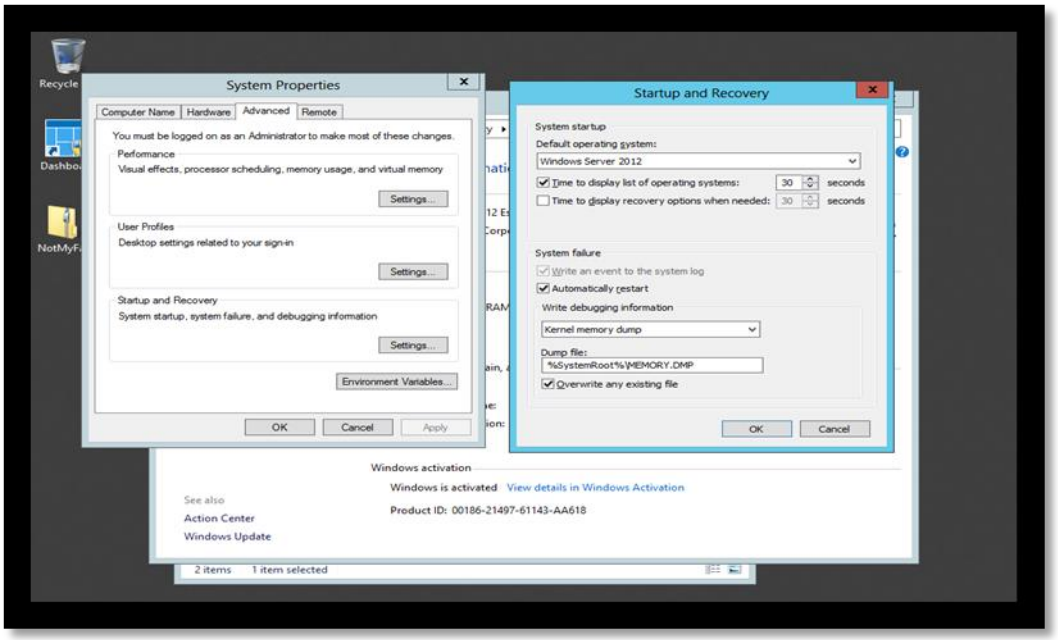
Patched file :



Un-patched files

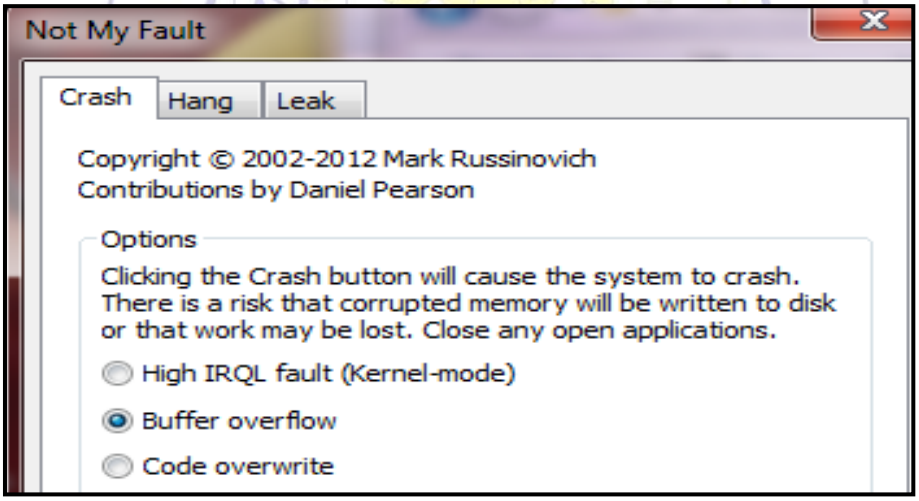


Since there is no evidence of concept accessible for the CVE-2016-7256, an appliance formed by Microsoft known as “not my fault” is employed to display memory leakage and is also used to create buffer overflow. Therefore, it will permit us to examine the role that influenced the function. The system is readied to get a memory dump that will be recovered and examined after the crash. Happened through a “not my fault” appliance. The following image demonstrates the setting up of the memory dump site.



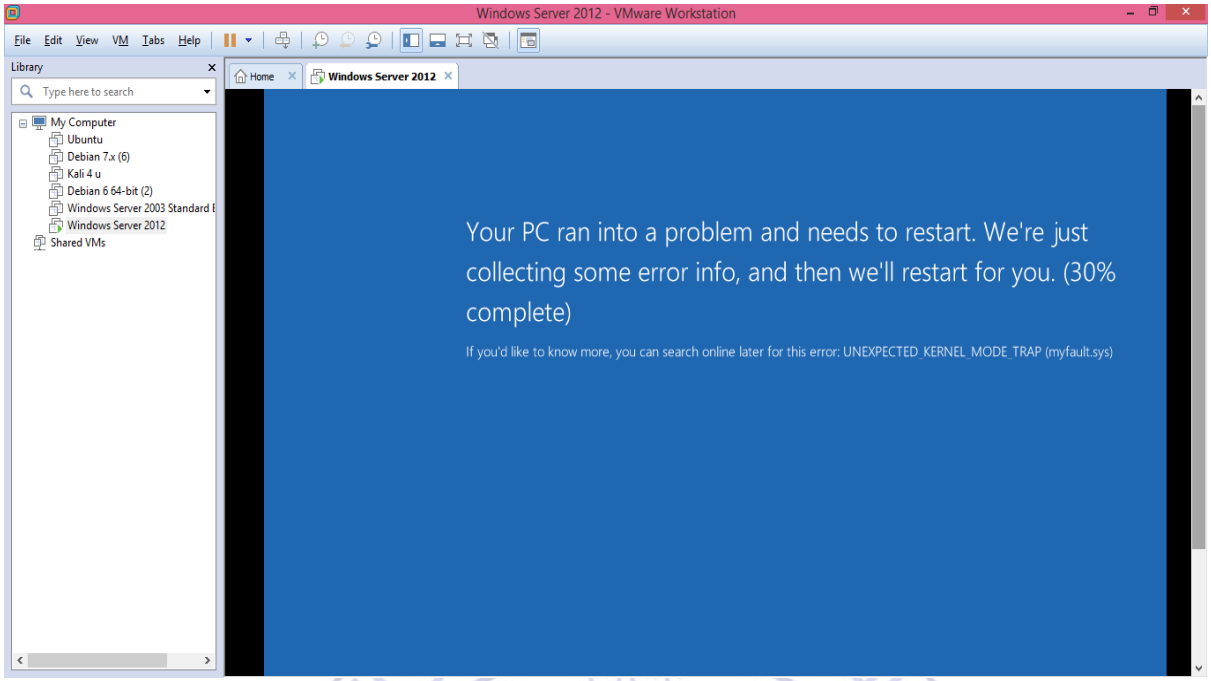
Figur2: setting up of the memory dump site.

The appliance “not my fault” is set to implement a buffer overflow. It can be observed in the following illustration.



Figur3: buffer overflow

When the system is restarted, the memory dump is recovered. At this instant, WINdbg is employed to examine the memory outflow. The following illustration shows that the dilemma results from (afd.sys Afd+267e3) as demonstrated**.**



CVE-2016-7256 exploit open kind font elevation of right:

In early June 2016, unknown actors started employing an implant known as "Henkray" within low-volume invasions that concentrated on destinations within South Korea. Afterwards, in November 2016, the font models discovered on involved computers were particularly manipulated

through hardcoded addresses and information to reproduce authentic kernel memory designs. This indicates the probability that a secondary device dynamically produced the exploit cypher at the moment of penetration.

Figure 4: Auto-generation of font files with an exploit

Utilizing profound forensic examination of the binary data discovered in specimens, we extorted the entire hardcoded offsets is established the kernel edition targeted through this exploit: Windows 8 64-bit by Microsoft Malware Protection Centre (2017).

2.2 Purpose table corruption for initial code implementation:

The font exploit employs ***fa_Callbacks*** to distort the operation table and attain the first code implementation. The callback is made for the CFF parsing purpose. The following snippet illustrates a corrupted ***ftell*** indicator to a ***nt!qsort+0x39*** position in kernel code.

```
kd> dt fa_Callbacks 0xfffff880`0514f380
ATMFD!fa_Callbacks
   +0x000 ctx              : 0x41414141`41414141 Void
   +0x008 fread            : 0x41414141`41414141     unsigned int64  +4141414141414141
   +0x010 fwrite           : 0x41414141`41414141     unsigned int64  +4141414141414141
   +0x018 fseek            : 0x41414141`41414141     int  +4141414141414141
   +0x020 ftell            : 0xfffff803`d28bacd9     long  +fffff803d28bacd9
   +0x028 allocate         : 0x41414141`41414141     void*  +4141414141414141
   +0x030 ATMfree          : 0x41414141`41414141     void  +4141414141414141
   +0x038 memcmp           : 0x41414141`41414141     int  +4141414141414141
   +0x040 memmove          : 0x41414141`41414141     void*  +4141414141414141
   +0x048 memset           : 0x41414141`41414141     void*  +4141414141414141
   +0x050 message          : 0x41414141`41414141     void  +4141414141414141
   +0x058 seed             : 0x90a4f3e6`014c5f50     long  +90a4f3e6014c5f50
   +0x060 strcmp           : 0x83485e00`000000e8     int  +83485e00000000e8
   +0x068 strlen           : 0x8d48504e`8b4838ec     int  +8d48504e8b4838ec
```

nt!qsort+0x39

Figure 5. fa-Callbacks table corruption

The subsequent snippet demonstrates the cypher that calls the corrupt purpose pointer resulting in a kernel ROP sequence.

```
ATMFD+0x3d6f5:
fffff960`00b786f5 ff5320          call    qword ptr [rbx+20h]
```

Figure 6: fa-Callbacks.ftell function call code

Once the corrupted role is called, the control leaps to the initial ROP device at nt!qsort+0x39 that fine-tunes the stack indicator and initializes several record values from stack values.

```
kd> u fffff800`3f484000+36CD9
nt!qsort+0x39:
fffff800`3f4bacd9 4881c418040000  add     rsp,418h
fffff800`3f4bace0 415e            pop     r14
fffff800`3f4bace2 415d            pop     r13
fffff800`3f4bace4 415c            pop     r12
fffff800`3f4bace6 5d              pop     rbp
fffff800`3f4bace7 c3              ret
```

Figure 7: First ROP gadget

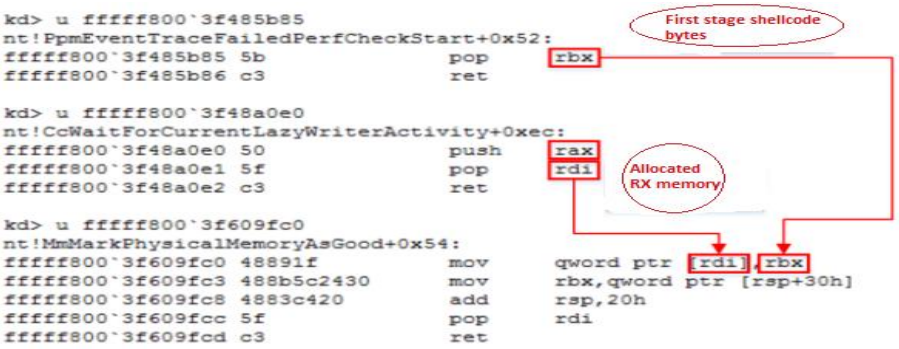


Figure 8: Copying the stage 1 shellcode

Following the first device, the stack identifies a kernel ROP chain that calls to Ex Allocate Pool with Tag call to preserve shellcode memory—an additional ROP. The device will duplicate the initial 8 bytes of the phase 1 shellcode to the allotted memory.

2.3Shellcode and rights escalation:

The phase 1 shellcode is extremely small. Its significant role is to duplicate the central body of the shellcode to recently assigned memory and operate them through a JMP RAX control relocation.

```
fffffa83`00a08000 50              push    rax
fffffa83`00a08001 5f              pop     rdi
fffffa83`00a08002 4c01e6          add     rsi,r12
fffffa83`00a08005 f3a4            rep movs byte ptr [rdi],byte ptr [rsi]
```

Figure 9. Stage 1 shellcode

The key shellcode runs following the copy guidelines. The major shellcode, as well as a small code piece, carries out a recognized token-stealing method. It subsequently duplicates the token indicator from a SYSTEM procedure to the target procedure, attaining privilege intensification. The SYSTEM procedure and destination procedure PIDs and specific offsets for the kernel APIs required by the shellcode are hardcoded within the font model.

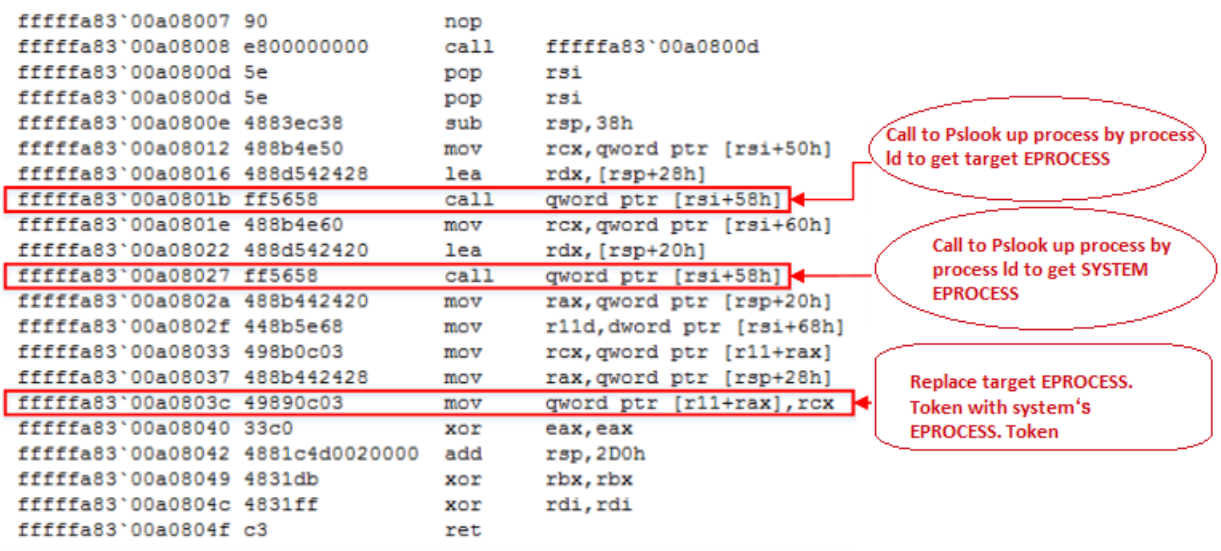


Figure 10: Token replacement technique

2.4 Mitigating font exploits with AppContainer :

Exploit alleviation methods within Windows 10 Anniversary Update that were made available months before these zero-day invasions managed to counteract the particular exploits and their

exploit techniques. Therefore these alleviation methods are considerably decreasing invasion surfaces that might have been accessible to upcoming zero-day exploits, according to Prabhu, V., Mengora, G., Ho, V., Moynihan, T., Prabhu, V. and Usman, M. (2017).

According to Brinkmann, M. (2017), while opening the spiteful font specimen on Windows 10 Anniversary Update, font parsing takes place wholly in AppContainer rather than the kernel. AppContainer offers a secluded sandbox that efficiently prevents font exploits (amid other exploits) from attaining escalated rights. The secluded sandbox significantly decreases font parsing as an invasion surface.

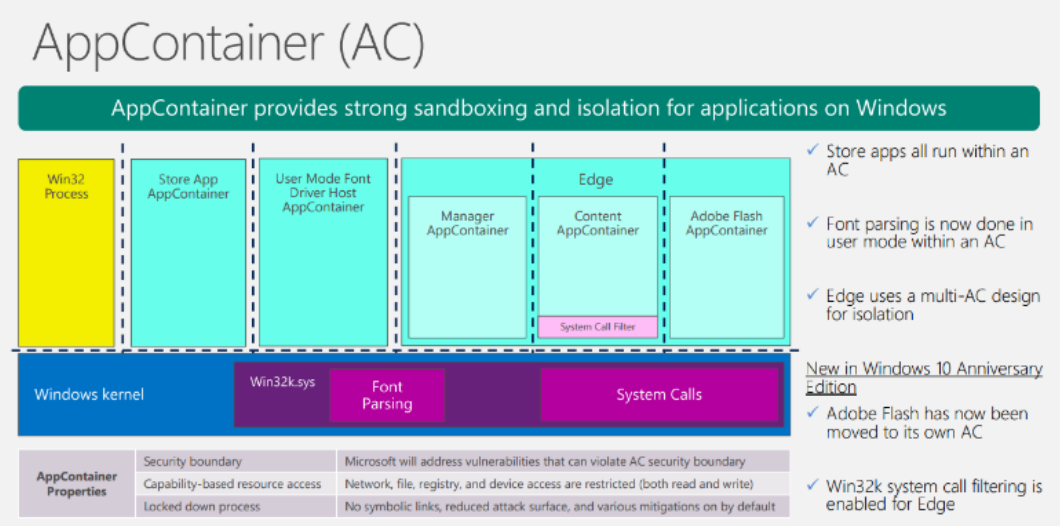


Figure 11: AppContainer protects against corrupted fonts in Windows 10 Anniversary Update

Moreover, Windows 10 Anniversary Update incorporates extra corroboration for font folder parsing. During our experiments, the particular exploit code for CVE-2016-7256 fails these tests and is incapable of arriving at vulnerable code.

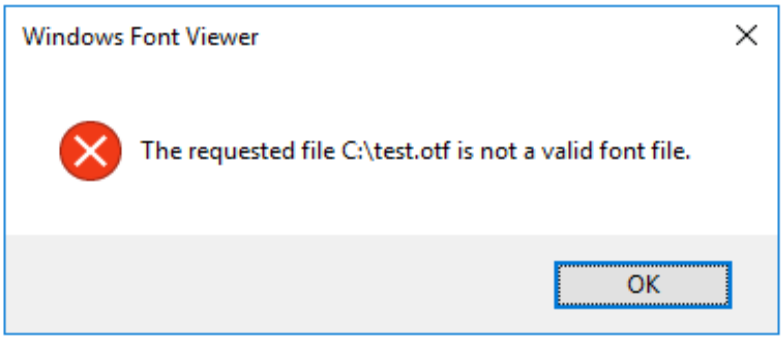


Figure 12. Windows 10 font viewer error

DISSCUSION

Threat of the vulnerability CVE- 2016-7256 to a network and domain:

Once the attacker convinces the user to open a document or a website with crafted fonts, he can exploit this vulnerability. Additionally, the attacker will use the privileges of the convinced user to execute the arbitrary code. For example, if the user is the domain administrator, the attacker will gain domain administrator rights and perform all the operations of the domain administrator. Such operations include changing system settings such as time, shutting computers remotely and halting company operations, loading and unloading device drivers, taking ownership of files and objects, managing, auditing, editing security codes, and accessing the web server. This implies that a company with an e-commerce website will see its customer information, including credit card information and bank details, according to Tenable.com.(2017).

The attacker can also host a malicious website in a web browser, and the virus will infect any user visiting that website. Additionally, attackers in the local base exploits can convince their targets to open email attachments that redirect them to malicious sites or attempt to get higher privileges. For the attackers to fully exploit the system, he has to get the system type, IP address, and other relevant information of the targeted user.To protect users against CVE, many strategies have to be used because users access different web pages. This can be done by deploying the relevant defence strategies, keeping abreast with Microsoft updates, putting systems for detection of attacker behaviour, and beefing up the security of the frequently targeted system by Eduard Kovacs (2016).

CONCLUSION

In summary, a details discussion of CVE-2016-7256 has been provided in this paper. The working of CVE and it is technical aspects and the danger that CVE vulnerability can cause are also explained. A practical demonstration of how CVE-2016-7256 work has been provided to make it easy for the user to understand. The paper has also addressed the working of MS16-132, which is the recommended solution by Microsoft.

The exploitation of this vulnerability, as presented in this paper, shows that the attacker can use it to get into the company system, take control, and execute malicious codes. The paper has also described how the attacker can induce a user to access a website to initiate the attack. Given that this vulnerability has different effects on different versions of Windows, the paper found it fit to describe its effect on different Windows versions. Also, this essay, Looked into current invasion campaigns entailing two zero-day kernel exploits. We observed the means exploit alleviation methods in Windows 10 Anniversary Update that was made available months before these zero-day invasions managed to counteract not just the particular exploits but also their exploit techniques. Therefore, these alleviation methods considerably decrease invasion surfaces that might have been accessible to upcoming zero-day exploits.

Lastly, ways of mitigating the vulnerabilities posed by CVE-2016-7256 are discussed from the user to the system administrator. Moreover, the system's security through the best server management has been explained in this paper.

Recommendations:

Once Google researchers discovered this vulnerability, Microsoft developed a solution in the form of a patch that the user has to apply to block the untrusted fonts. The patch can be found under Blocking of untrusted Fonts in an Enterprise. Microsoft also developed a function in its Windows OS to allow system administrators to block fonts which are not trusted. Once the administrator activates this feature, other users cannot load untrusted fonts and thus reducing the risk of attack on an organisational system, according to Parrish,k(2017). The Microsoft Baseline Security Analyzer (MBSA) also allows system administrators to scan local and remote systems for missing security system updates and misconfiguration. Organisations can further protect their systems by using penetration services from pen-testing companies to protect themselves from such vulnerabilities. Further, only trustworthy people should be given access to a company's computer network to reduce cases of malicious people exploiting an organisation using this type of vulnerability through executing arbitrary codes and accessing files with untrusted fonts.

ACKNOWLEDGEMENT

I am indebted to my father, Faraj Hwedi, for his continued guidance and endless supply of fascination. His direct approach to research and science is a source of inspiration. Computers did most of the work in this thesis (they never get their due credit). I also had the pleasure of working with my friend, Ashraf Mohamed.
Most importantly, I am grateful for my family's unconditional, unequivocal, and loving support.

References

1. Akram, J., & Luo, P. (2021). SQVDT: A scalable quantitative vulnerability detection technique for source code security assessment. *Software: Practice and Experience*, 51(2), 294-318. https://doi.org/10.1002/spe.2905.
2. Animesh Jain, V.S.P.M. (2022) Microsoft released out-of-band advisory – windows adobe type manager library remote code execution vulnerability (ADV200006), Qualys Security Blog. Available at: https://blog.qualys.com/vulnerabilities-threat-research/2020/03/23/microsoft-released-out-of-band-advisory-microsoft-windows-adobe-type-manager-library-remote-code-execution-vulnerability-adv200006
3. BARANOV, (2016). [online] Available at: http://www.welivesecurity.com/wpcontent/uploads/2017/01/Windows-Exploitation-2016-A4.pdf .
4. Brinkmann, M. (2017). Microsoft: Windows 10 hardening against 0-day exploits - gHacks Tech News. [online] gHacks Technology News. Available at: https://www.ghacks.net/2017/01/18/microsoft-windows-10-hardening-against-0-day-exploits/ .
5. Davis, M., Bodmer, S. and Lemasters, A. (2010) Hacking Exposed Malware and Rootkits Reviews: Malware and Rootkits Security Secrets and Solutions. The New York: McGraw-Hill Companies, Inc.
6. Davis, M., Bodmer, S., & LeMasters, A. (2009). Hacking exposed malware and rootkits. McGraw-Hill, Inc..

7. Domars (2022) Debugging tools for windows (WinDbg, KD, CDB, NTSD) - windows drivers, Windows drivers | Microsoft Learn. Available at: https://learn.microsoft.com/en-us/windows-hardware/drivers/debugger/.
8. Eduard Kovacs (2016). Microsoft Patches Windows Zero-Day Exploited by Russian Hackers | SecurityWeek.Com. [online] Available at: http://www.securityweek.com/microsoft-patches-windows-zero-day-exploited-russian-hackers .
9. Joh, H. and Malaiya, Y. K. (2010) A Framework for Software Security Risk Evaluation Using the Vulnerability Lifecycle and CVSS Metrics. [Online].
10. Kaspersky (2015) Multiple vulnerabilities in Microsoft Windows. AO Kaspersky Lab. [Online]. Available at: http://securelist.social-kaspersky.com/en/kadvisories/KLA10694.
11. Microsoft (2015). Install Windows updates in Windows 7.[WWW].Available at:http://windows.microsoft.com/en-us/windows7/install-windows-updates [Accessed 25 Jan 2017].
12. Microsoft (2016). *Microsoft Security Bulletin MS16-132 - Critical*. [online] Available at: http://technet.microsoft.com/en-us/security/bulletin/ms16-132 [Accessed 22Jan. 2017].
13. Microsoft Malware Protection Center. (2017). Hardening Windows 10 with zero-day exploit mitigations. [online] Available at: https://blogs.technet.microsoft.com/mmpc/2017/01/13/hardening-windows-10-with-zero-day-exploit-mitigations/ .
14. Moran, A. T. (2012) *Assessing and Extending the Common Vulnerability Scoring System*. Master Thesis, University of London.
15. Msdn.microsoft.com. (2016). Debugging Tools for Windows (WinDbg, KD, CDB, NTSD) - Windows 10 hardware dev. [online] Available at: https://msdn.microsoft.com/en-gb/library/windows/hardware/ff551063(v=vs.85).aspx .
16. NVD NIST (2016). *NVD - Detail*. [online] Available at: https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2016-7256 .
17. Parrish, K. (2017). Microsoft releases patch for zero-day Flash and Windows Kernel exploit. [online] Digital Trends. Available at: http://www.digitaltrends.com/computing/google-warns-microsoft-no-windows-fix-yet/ .
18. Prabhu, V., Mengora, G., Ho, V., Moynihan, T., Prabhu, V. and Usman, M. (2017). Windows 10 | A Box in Space. [online] Myspacebox.net. Available at: https://www.myspacebox.net:8443/category/windows-10/ .
19. Symantec (2017). Symantec Intelligence Report: October 2015. [online] Available at:https://www.symantec.com/connect/blogs/symantec-intelligence-report-october-2015 .
20. Tang, J. (2016). A Look at the OpenType Font Manager Vulnerability from the Hacking Team Leak - TrendLabs Security Intelligence Blog. [online] TrendLabs Security Intelligence Blog. Available at: http://blog.trendmicro.com/trendlabs-security-intelligence/a-look-at-the-open-type-font-manager-vulnerability-from-the-hacking-team-leak/ [Accessed 29 Jan. 2017].
21. Tenable.com. (2017). Nessus Plugins. [online] Available at: https://www.tenable.com/plugins/index.php?view=single&id=94633.