Ejercicio: Verónica Franco

- **CVE-2017-11882 - María Verónica Franco**

Recopila la siguiente información sobre la vulnerabilidad o boletín correspondiente

- **Alias (si tiene)**

Microsoft Office memory corruption vulnerability

- **Fecha de publicación Código CVE**

La fechad e publicacion es 14/11/2017, pero a partir de esa fecha se han hecho 14 modificaciones hasta 2021.

- **Código CWE**

CWE-119 Restricción incorrecta de operaciones dentro de los límites de un búfer de memoria

- **Código CVSS explicado por partes, tanto número como cada uno de los campos**

CVSS Version 3.0 y CVSS Version 3.1: Con estas métricas veremos numéricamente la gravedad del fallo.

La puntuación base es 7.8, este score permite conocer el grado de vulnerabilidad del ataque, es calculado en base a métricas y puede diferir se acuerdo a los sistemas operativos ya que cada uno de estos van actualizando versiones e incluyen mas protección.

METRICAS DE PUNTUACION DE BASE

METRICAS DE EXPLOTABILIDAD: 5.9 puntos

En este caso 7.8 es una puntuación base y viene dado porque en primer lugar el

vector de ataque es local, es decir, la vulnerabilidad no esta vinculada con la red, el atacante debe estar aprovechando la vulnerabilidad localmente y muchas veces depende de la interacción con el usuario. Por otro lado,

la complejidad del ataque es baja, esto significa que no hay muchos obstáculos para el atacante para explotar la vulnerabilidad, en cuanto a los

privilegios requeridos, ninguno; para el ataque es ninguno, esto quiere decir que no hay que realizar configuración ni acceso para llevar a cabo el ataque.

Interacción con el usuario, **requerido**, la interacción con usuario como mencione anteriormente es necesaria, el atacante depende de esa interacción.

Scope, Unchanged: esto significa que la vulnerabilidad explotada solo puede afectar recursos manejados por una autoridad similar, es decir que el componente vulnerable y el componente de impacto son iguales.

METRICAS DE IMPACTO: 1.8 puntos

Impacto a la confidencialidad: es alto, es decir los datos pueden ser fácilmente accesados y la privacidad es baja.

Impacto a la integridad: es alto, los datos pueden ser fácilmente modificados.

Impacto a la disponibilidad: es alto, la información esta disponible para su acceso.

METRICAS DE PUNTUACION TEMPORAL

Se calcula en base a la puntuación base.

MADUREZ DEL CODIGO DE EXPLOTACION: no definido, no influye en la puntuacion

NIVEL DE REMEDIACION: no definido, no influye en la puntuacion

INFORME DE CONFIANZA: no definido, no influye en la puntuación

METRICAS DE PUNTUACION AMBIENTAL:

METRICAS DE EXPLOTABILIDAD

Vector de ataque: modificación no definida.

Complejidad de ataque: modificación no definida.

Privilegios requeridos: modificación no definida.

Interacción con el usuario: modificación no definida.

Escape: modificación no definida.

METRICAS DE IMPACTO

Impacto a la confidencialidad: modificación no definida.

Impacto a la integridad: modificación no definida.

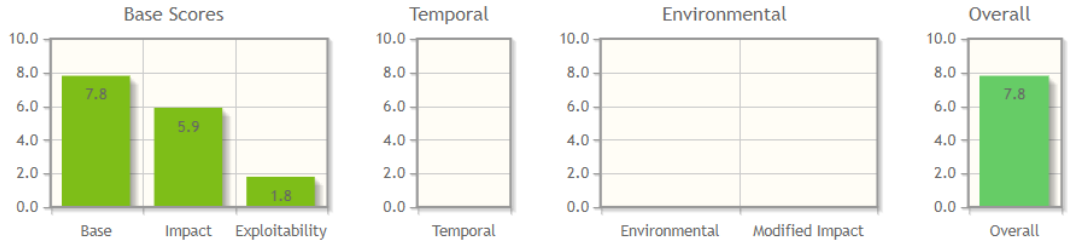
Impacto a la disponibilidad: modificación no definida.

MODIFICADORES DE SUBPUNTUACION DE IMPACTO

Requerimiento de confidencialidad: modificación no definida.

Requerimiento de integridad: modificación no definida.

Requerimiento de disponibilidad: modificación no definida.



Base Score Metrics

Exploitability Metrics

Attack Vector (AV)*

Network (AV:N) | Adjacent Network (AV:A) | **Local (AV:L)** | Physical (AV:P)

Attack Complexity (AC)*

Low (AC:L) | High (AC:H)

Privileges Required (PR)*

None (PR:N) | Low (PR:L) | High (PR:H)

User Interaction (UI)*

None (UI:N) | **Required (UI:R)**

Scope (S)*

Unchanged (S:U) | Changed (S:C)

Impact Metrics

Confidentiality Impact (C)*

None (C:N) | Low (C:L) | **High (C:H)**

Integrity Impact (I)*

None (I:N) | Low (I:L) | **High (I:H)**

Availability Impact (A)*

None (A:N) | Low (A:L) | **High (A:H)**

Temporal Score Metrics

Exploit Code Maturity (E)

Not Defined (E:X) | Unproven that exploit exists (E:U) | Proof of concept code (E:P) | Functional exploit exists (E:F) | High (E:H)

Remediation Level (RL)

Not Defined (RL:X) | Official fix (RL:O) | Temporary fix (RL:T) | Workaround (RL:W) | Unavailable (RL:U)

Report Confidence (RC)

Not Defined (RC:X) | Unknown (RC:U) | Reasonable (RC:R) | Confirmed (RC:C)

Environmental Score Metrics

Exploitability Metrics

Attack Vector (MAV)

Not Defined (MAV:X) | Network (MAV:N) | Adjacent Network (MAV:A) | Local (MAV:L) | Physical (MAV:P)

Attack Complexity (MAC)

Not Defined (MAC:X) | Low (MAC:L) | High (MAC:H)

Privileges Required (MPR)

Not Defined (MPR:X) | None (MPR:N) | Low (MPR:L) | High (MPR:H)

User Interaction (MUI)

Not Defined (MUI:X) | None (MUI:N) | Required (MUI:R)

Scope (MS)

Not Defined (MS:X) | Unchanged (MS:U) | Changed (MS:C)

Impact Metrics

Confidentiality Impact (MC)

Not Defined (MC:X) | None (MC:N) | Low (MC:L) | High (MC:H)

Integrity Impact (MI)

Not Defined (MI:X) | None (MI:N) | Low (MI:L) | High (MI:H)

Availability Impact (MA)

Not Defined (MA:X) | None (MA:N) | Low (MA:L) | High (MA:H)

Impact Subscore Modifiers

Confidentiality Requirement (CR)

Not Defined (CR:X) | Low (CR:L) | Medium (CR:M) | High (CR:H)

Integrity Requirement (IR)

Not Defined (IR:X) | Low (IR:L) | Medium (IR:M) | High (IR:H)

Availability Requirement (AR)

Not Defined (AR:X) | Low (AR:L) | Medium (AR:M) | High (AR:H)

CVSS Version 2.0: Con estas métricas veremos numéricamente la gravedad del fallo.

La puntuación base es de 9.3, mas alta que las versiones anteriormente expuestas (versión 3.0 y versión 3.1). Esto debido a que la subpuntuacion de impacto es de 10.00 u la subpuntuacion de explotabilidad es 8.6 y el promedio entre ambos nos da la puntuación base.

METRICAS DE PUNTUACION BASE

METRICAS DE EXPLOTABILIDAD: la puntuación de esta metrica es de 8.6 esto debido a los siguientes ítems

Vector de acceso: red: el ataque puede realizarse a la red por lo que el atacante no necesita encontrarse en el lugar ni cercano al objetivo, puede llevar a cabo sus acciones remotamente lo que hace mas peligroso el acceso.

Complejidad de acceso: medio, para el atacante el acceso al objetivo no es totalmente fácil, por lo que debe haber realizado una investigación previa y tener reunida alguna información a parte de tener conocimientos de ingeniería social para que su ataque sea exitoso.

Autenticación: ninguna; no se necesita ninguna autenticación para acceder y explotar la vulnerabilidad.

METRICAS DE IMPACTO: la puntuación es de 10.00, es decir se cumplen todas las métricas.

METRICAS DE PUNTUACION TEMPORAL

Se calcula en base a la puntuación base.

MADUREZ DEL CODIGO DE EXPLOTACION: no definido, no influye en la puntuacion

NIVEL DE REMEDIACION: no definido, no influye en la puntuacion

INFORME DE CONFIANZA: no definido, no influye en la puntuación

METRICAS DE PUNTUACION AMBIENTAL:

MODIFICADORES GENERALES

Potencial de daños colaterales: no definido, no influye en la puntuación

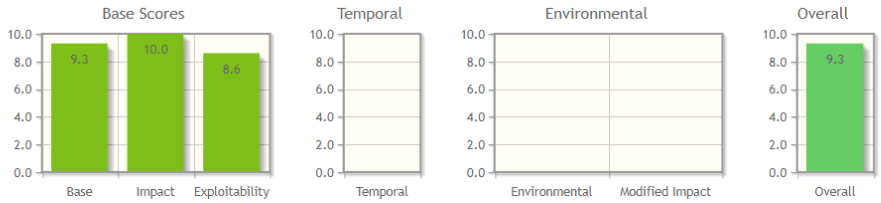
Distribución objetivo: **:** no definido, no influye en la puntuación

MODIFICADORES SUBPUNTUACION DE IMPACTO

Requerimiento de confidencialidad: no definido, no influye en la puntuación

Requerimiento de integridad: no definido, no influye en la puntuación

Requerimiento de disponibilidad: no definido, no influye en la puntuación



CVSS Base Score: 9.3
Impact Subscore: 10.0
Exploitability Subscore: 8.6
CVSS Temporal Score: NA
CVSS Environmental Score: NA
Modified Impact Subscore: NA
Overall CVSS Score: 9.3

Base Score Metrics

Exploitability Metrics

Access Vector (AV)*

Local (AV:L) | Adjacent Network (AV:A) | **Network (AV:N)**

Access Complexity (AC)*

High (AC:H) | **Medium (AC:M)** | Low (AC:L)

Authentication (Au)*

Multiple (Au:M) | Single (Au:S) | **None (Au:N)**

Impact Metrics

Confidentiality Impact (C)*

None (C:N) | Partial (C:P) | **Complete (C:C)**

Integrity Impact (I)*

None (I:N) | Partial (I:P) | **Complete (I:C)**

Availability Impact (A)*

None (A:N) | Partial (A:P) | **Complete (A:C)**

Temporal Score Metrics

Exploitability (E)

Not Defined (E:ND) | Unproven that exploit exists (E:U) | Proof of concept code (E:POC) | Functional exploit exists (E:F) | High (E:H)

Remediation Level (RL)

Not Defined (RL:ND) | Official fix (RL:OF) | Temporary fix (RL:TF) | Workaround (RL:W) | Unavailable (RL:U)

Report Confidence (RC)

Not Defined (RC:ND) | Unconfirmed (RC:UC) | Uncorroborated (RC:UR) | Confirmed (RC:C)

Environmental Score Metrics

General Modifiers

Collateral Damage Potential (CDP)

Not Defined (CDP:ND) | None (CDP:N) | Low (light loss) (CDP:L) | Low-Medium (CDP:LM) | Medium-High (CDP:MH) | High (catastrophic loss) (CDP:H)

Target Distribution (TD)

Not Defined (TD:ND) | None [0%] (TD:N) | Low [0-25%] (TD:L) | Medium [26-75%] (TD:M) | High [76-100%] (TD:H)

Impact Subscore Modifiers

Confidentiality Requirement (CR)

Not Defined (CR:ND) | Low (CR:L) | Medium (CR:M) | High (CR:H)

Integrity Requirement (IR)

Not Defined (IR:ND) | Low (IR:L) | Medium (IR:M) | High (IR:H)

Availability Requirement (AR)

Not Defined (AR:ND) | Low (AR:L) | Medium (AR:M) | High (AR:H)

- Boletín de seguridad que se publicó (si es que se incluyó en alguno)

https://msrc.microsoft.com/update-guide/en-US/vulnerability/CVE-2017-11882

https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-11882

- **Dirección de documentación con el paper / artículo correspondiente al CVE**

https://msrc.microsoft.com/update-guide/en-US/vulnerability/CVE-2017-11882

https://www.trendmicro.com/vinfo/us/security/news/vulnerabilities-and-exploits/17-year-old-ms-office-flaw-cve-2017-11882-actively-exploited-in-the-wild

https://www.rapid7.com/db/vulnerabilities/msft-cve-2017-11882/

https://unit42.paloaltonetworks.com/unit42-analysis-of-cve-2017-11882-exploit-in-the-wild/

https://github.com/unamer/CVE-2017-11882

https://www.fortinet.com/blog/threat-research/excel-document-delivers-malware-by-exploiting-cve-2017-11882

https://cve.mitre.org/cgi-bin/cvename.cgi?name=cve-2017-11882

https://securityaffairs.co/wordpress/86886/hacking/microsoft-cve-2017-11882-flaw-attacks.html

https://www.incibe-cert.es/alerta-temprana/vulnerabilidades/cve-2017-11882

https://sensorstechforum.com/es/cve-2017-11882-still-used-hackers/

https://www.escudodigital.com/ciberseguridad/malware-formbook-sigue-acecho-aprovecha-vulnerabilidad-office-activa-2017_51752_102.html

https://www.seguridad.unam.mx/microsoft-corrige-20-vulnerabilidades-criticas

https://fwhibbit.es/explotando-vulnerabilidades-cve-2017-11882

https://learn.microsoft.com/es-es/officeupdates/semi-annual-channel-2017

https://news.sophos.com/es-es/2019/07/29/microsoft-advierte-sobre-el-exploit-de-la-ecuacion-del-viaje-en-el-tiempo-estas-a-salvo/

https://statistics.securelist.com/es/country/dominican%20republic/vulnerability-scan/week

https://threats.kaspersky.com/mx/threat/Exploit.Win32.CVE-2017-11882/

- **Software que afecta (qué software es, qué version o versiones)**

Microsoft Office 2007 Service Pack 3, Microsoft Office 2010 Service Pack 2, Microsoft Office 2013 Service Pack 1 y Microsoft Office 2016 permiten a un atacante ejecutar código arbitrario en el contexto del usuario actual al no poder manejar correctamente los objetos en la memoria, también conocido como " Vulnerabilidad de daños en la memoria de Microsoft Office".

Microsoft Office 2007 Service Pack 3

Microsoft Office 2010 Service Pack 2 (32-bit editions)

Microsoft Office 2013 Service Pack 1 (64-bit editions)

Microsoft Office 2016 (32-bit edition)

Microsoft Office 2013 Service Pack 1 (32-bit editions)

Microsoft Office 2010 Service Pack 2 (64-bit editions)

Microsoft Office 2016 (64-bit edition)

- **Descripción de la vulnerabilidad**

CVE-2017-11882 es un problema de corrupción de memoria de 17 años en Microsoft Office (incluido Office 360). Cuando se explota con éxito, puede permitir que los atacantes ejecuten código remoto en una máquina vulnerable, incluso sin la interacción del usuario, después de abrir un documento malicioso. La falla reside en el Editor de ecuaciones (EQNEDT32.EXE), un componente de Microsoft Office que inserta o edita objetos de vinculación e incrustación de objetos (OLE) en los documentos. Se lanzó públicamente un exploit de prueba de concepto, pero esto se solucionó con el martes de parches de noviembre de Microsoft.

- **Repercusiones a nivel mundial y curiosidades (botnets, ransomware, temas masivos, si están entre las más utilizadas a día de hoy…) y por qué creéis que es importante o porque creéis que no.**

Teniendo en cuenta que se trata de un software que explota la vulnerabilidad de Microsoft Office, por ende posee bastante repercusión a partir de 2017, sin embargo a la fecha este ataque ya fue parcheado, pero si hay atacantes que siguen utilizándolo para realizar ataques.

Tiempo después de que Microsoft haya parcheado la vulnerabilidad, Fortine hizo hallazgos, el malware que explota esta vulnerabilidad se estaba distribuyendo como un documento RTF, se distribuye como un archivo adjunto descargable desde un sitio web.

A partir de allí en 2018, no se han descubierto mas hallazgos, no obstante aparentemente este exploit ha sido reparado.