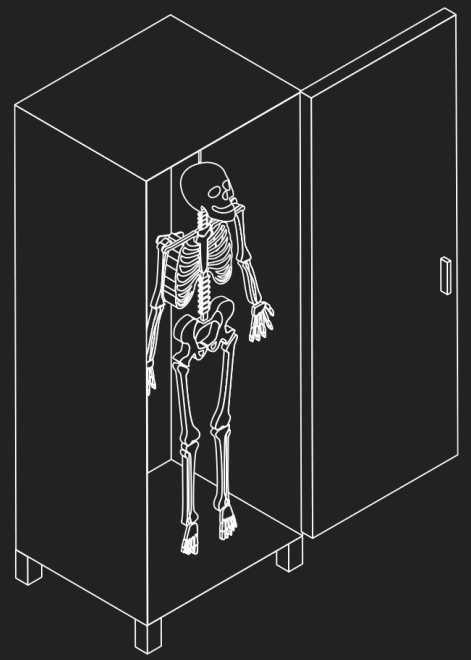
SKELETON IN THE CLOSET

La vulnerabilidad de MS Office que no conocías.

CVE-2017-11882



EMBEDI

INTRODUCCIÓN

Introducción

- Vulnerabilidades en bibliotecas de terceros utilizadas en software desactualizado.
- Código heredado y de terceros.
- Desarrollado en la prehistoria, cuando nadie seguía las pautas de desarrollo seguro.
- Código fuente se ha perdido y solo quedan binarios.

ETAPA PREPARATORIA Y METODOLOGÍA

Etapa preparatoria y metodología

- Office Suite: esta superficie de ataque sirve como prueba de fuego para definir:
  - Qué elementos de MS Office Suite pueden ser atacados.
  - Qué métodos puede utilizar un ciberdelincuente para realizar un ataque con éxito.
  - Qué módulos de MS Office Suite son responsables de manejar formatos y diferentes segmentos de documentos.
- Búsqueda tiene como objetivo identificar los módulos ejecutables con el menor número de funciones de seguridad habilitadas que protegen contra vulnerabilidades binarias.

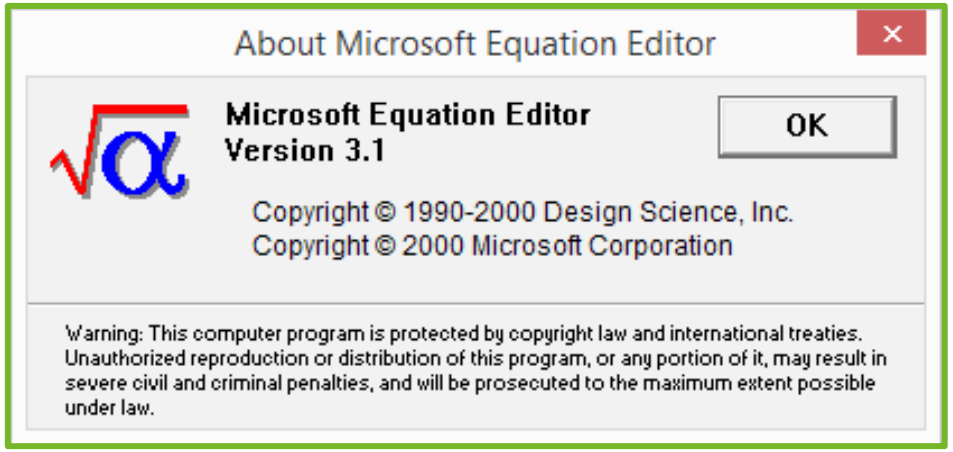
Etapa preparatoria y metodología

- *BinScope* útil para detectar debilidades de seguridad en los binarios.
- Permiten detectar componentes peligrosos, obsoletos y de terceros.
- Ensamblados sin mitigación de seguridad.
- La seguridad global de un sistema depende de su elemento mas débil.

Etapa preparatoria y metodología

- Resumen de los componentes más obsoletos de Microsoft Office 2016 x86:

1. Editor de ecuaciones de Microsoft (compilado sin las medidas de protección esenciales).
2. Controladores ODBC y bibliotecas Redshift (compilados sin medidas de protección esenciales).
3. Controladores ODBC y bibliotecas de Salesforce (compilados sin medidas de protección esenciales).
4. Algunas compilaciones .net responsables de la interfaz de usuario de Microsoft Office.



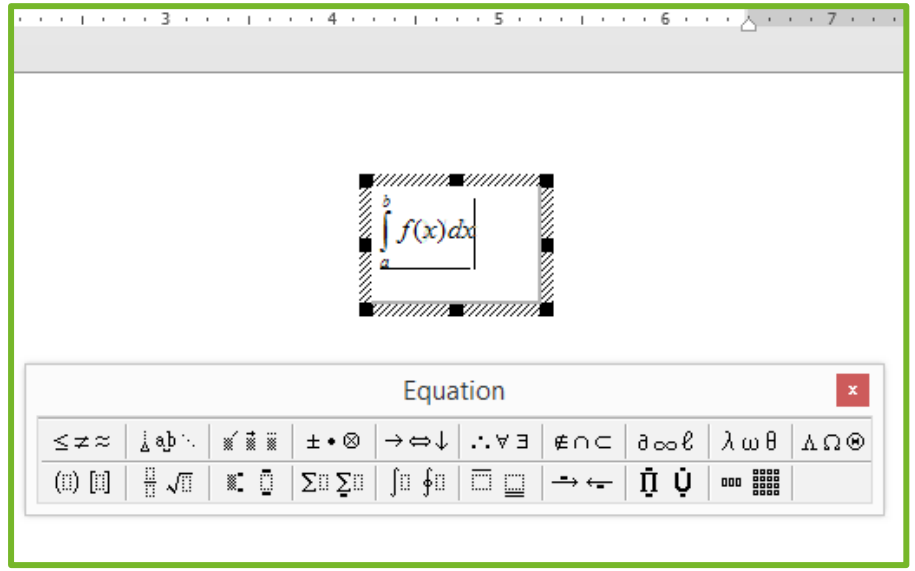
Etapa preparatoria y metodología

- BinScope identificó el módulo ejecutable EQNEDT32.EXE
- Se compiló el 9/11/2000.
- Desarrollado por Design Science Inc.
- Binscope marca EQNEDT32.EXE como un componente inseguro.

EQNEDT32.EXE HISTORIA DEL CASO

EQNEDT32.EXE. Historia del caso

- El componente es la inserción y edición de ecuaciones en documentos.
- Cualquier fórmula insertada en un documento es un objeto OLE.
- A partir del paquete de Microsoft Office 2007, los métodos de visualización y edición de ecuaciones cambiaron y el componente quedó desactualizado.
- No se eliminó del paquete, probablemente para garantizar compatibilidad con documentos anteriores.
- Es un servidor COM de OutProc ejecutado en un espacio de direcciones separado.

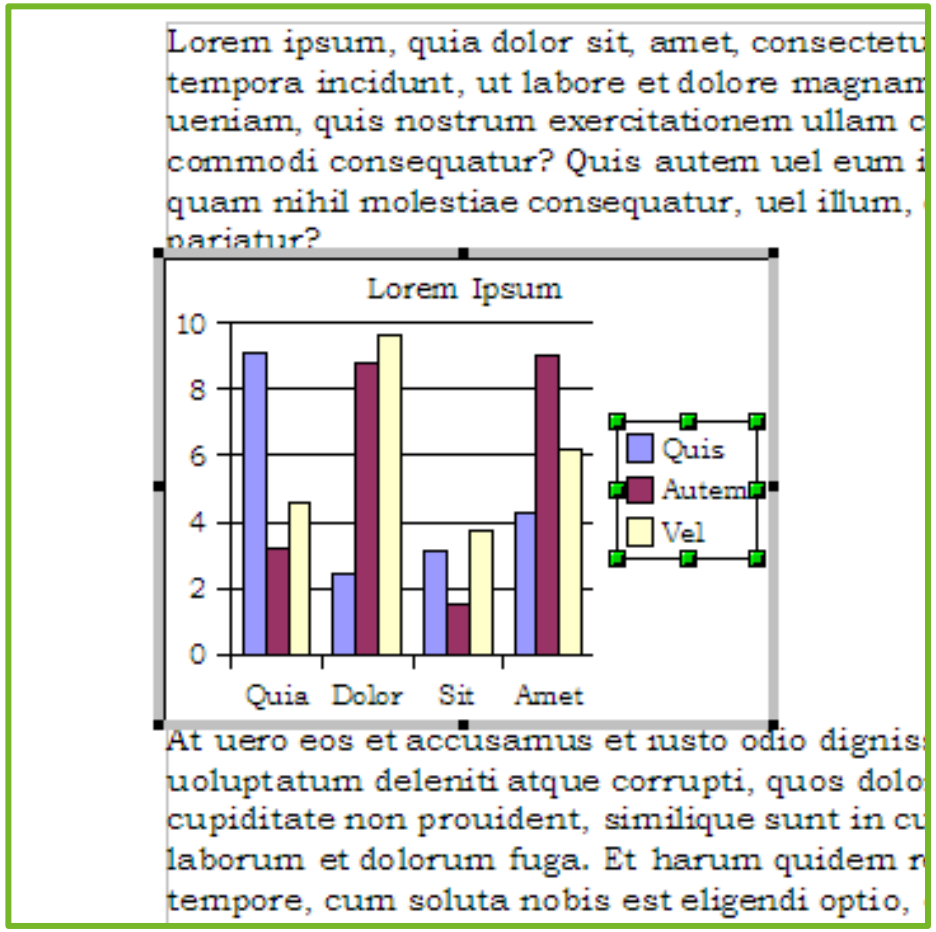


Process	CPU	Private Bytes	Working Set	PID	Description
System Idle Process	93.45	0 K	4 K	0	
System	0.22	1,688 K	12,856 K	4	
Interrupts	0.51	0 K	0 K	n/a	Hardware Interrupts and DPCs
smss.exe		312 K	1,052 K	408	Windows Session Manager
csrss.exe		2,968 K	5,744 K	580	Client Server Runtime Process
wininit.exe		936 K	4,044 K	676	Windows Start-Up Application
services.exe		4,160 K	7,464 K	736	Services and Controller app
svchost.exe		7,216 K	14,728 K	864	Host Process for Windows Services
dllhost.exe		1,324 K	5,980 K	3684	COM Surrogate
rundll32.exe	< 0.01	1,984 K	10,568 K	4288	Windows host process (Rundll32)
RuntimeBroker.exe		1,448 K	6,312 K	7972	Runtime Broker
SkypeBrowserHost.exe	< 0.01	14,568 K	31,792 K	7960	Skype Browser Host
wsmprovhost.exe	< 0.01	1,360 K	5,604 K	7352	Host process for WinRM plug-ins
EQNEDT32.EXE	< 0.01	1,904 K	8,448 K	8572	Microsoft Equation Editor
WmiPrvSE.exe		2,028 K	6,124 K	8408	WMI Provider Host
svchost.exe	< 0.01	6,300 K	10,848 K	896	Host Process for Windows Services

Los mecanismos y políticas de seguridad de los procesos de office no afectan la explotación de la vulnerabilidad.

La tecnología OLE en pocas palabras

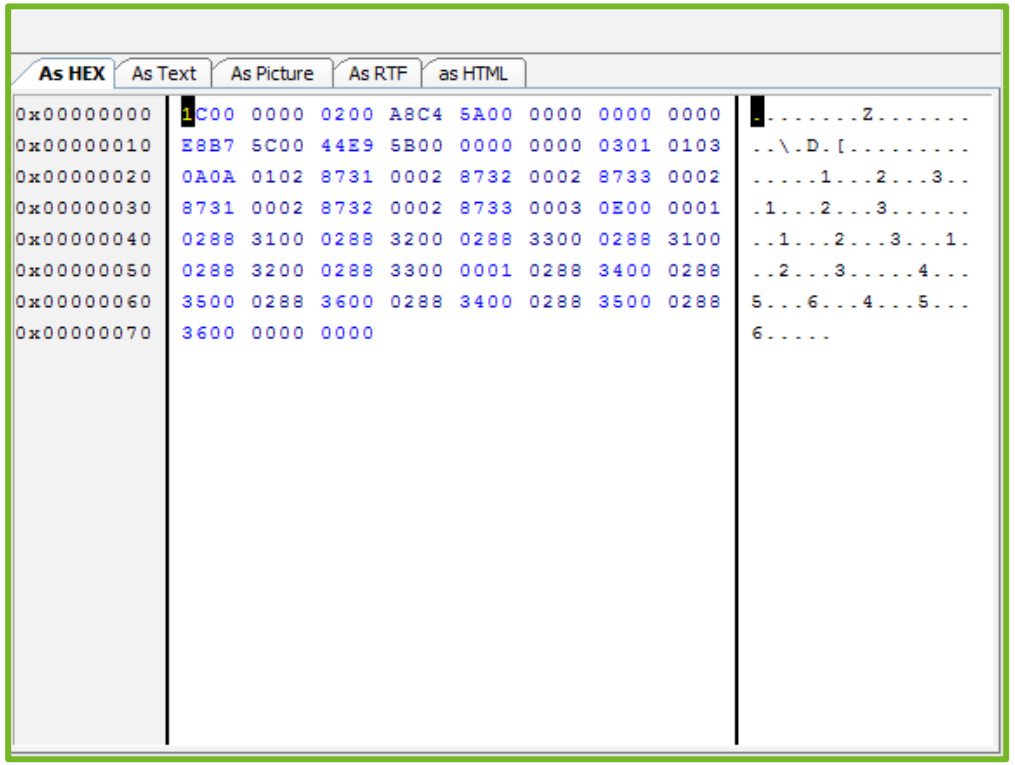
- Hay dos partes en un objeto OLE incrustado en un documento:
  - datos internos
  - una imagen que se muestra en el lugar de un objeto incrustado en un documento
- Procedimiento de carga de OLE desde datos internos. El procedimiento se lleva a cabo con la ayuda de los métodos *IPersistStorage* de la interfaz COM.



Análisis de EQNEDT32.exe

- EQNEDT32.EXE emplea un conjunto de interfaces COM estándar para OLE:
  - IOleObject
  - IDataObject
  - IOleInPlaceObject
  - IOleInPlaceActiveObject
  - IPersistStorage
- El método Load de IPersistStorage es el más prometedor para encontrar vulnerabilidades.
- El uso de técnicas simples de ingeniería inversa, es posible encontrar el método IPersistStorage::Load.

Análisis de EQNEDT32.exe



- El componente que los datos internos de la ecuación se pueden describir de la siguiente manera:

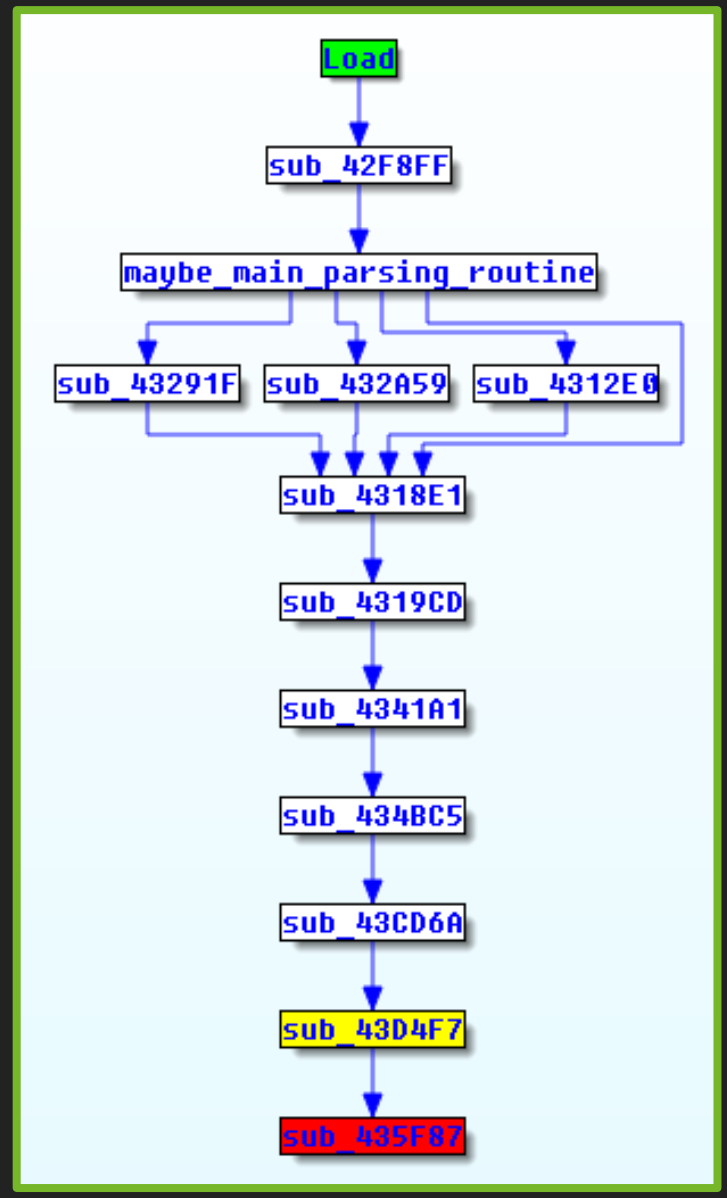
1. Tamaño del encabezado (2 bytes).
2. Campo de formulario del tamaño máximo de ecuación (4 bytes).
3. Encabezado con información sobre la estructura de la ecuación (24 bytes).
4. Representación interna de longitud arbitraria, que consta de símbolos y etiquetas elementales, de la ecuación.

Análisis de EQNEDT32.exe

- Complicado en la investigación fue definir el procedimiento principal que consistía en analizar el formulario de ecuación más difícil porque la copia y el guardado del formulario interno en la memoria global de HGLOBAL se realizaron con la ayuda de objetos globales con numerosas referencias a ellos
- El problema se resolvió creando dos coberturas de código, utilizando el instrumento DBI drcov (una parte del marco DynamoRIO1), para procesar dos ecuaciones diferentes. La ración de cobertura se calculó con la ayuda del lighthouse plug-in para IDA PRO.

Coverage %	Function Name	Address	Blocks Hit	Instructions Hit	Function Size
100.00%	sub_41618F	0x41618F	4 / 4	16 / 16	34
100.00%	sub_436111	0x436111	2 / 2	21 / 21	44
100.00%	sub_42B124	0x42B124	1 / 1	26 / 26	74
100.00%	sub_435DAA	0x435DAA	2 / 2	40 / 40	109
100.00%	sub_435F87	0x435F87	2 / 2	24 / 24	60
100.00%	sub_430DB1	0x430DB1	1 / 1	18 / 18	31
100.00%	sub_43C03E	0x43C03E	2 / 2	17 / 17	35
100.00%	sub_42B0D8	0x42B0D8	1 / 1	27 / 27	76
100.00%	sub_43B858	0x43B858	4 / 4	54 / 54	145
100.00%	sub_4400F0	0x4400F0	1 / 1	54 / 54	144
98.75%	sub_435CC1	0x435CC1	4 / 5	79 / 80	233
96.55%	sub_4366A1	0x4366A1	8 / 9	28 / 29	98
95.83%	sub_43C061	0x43C061	4 / 5	23 / 24	60
95.24%	sub_440807	0x440807	11 / 13	40 / 42	146
94.12%	sub_42D254	0x42D254	7 / 8	32 / 34	106
93.94%	sub_42BC8C	0x42BC8C	3 / 4	31 / 33	93
93.75%	sub_4407A5	0x4407A5	5 / 6	30 / 32	98
92.86%	sub_42B16E	0x42B16E	4 / 6	65 / 70	220
92.24%	sub_43B8E9	0x43B8E9	8 / 10	107 / 116	345
91.23%	sub_436452	0x436452	6 / 9	52 / 57	200
90.91%	sub_43593A	0x43593A	4 / 5	20 / 22	53
90.91%	sub_42AC56	0x42AC56	3 / 4	40 / 44	122
89.66%	sub_42D2BE	0x42D2BE	6 / 7	26 / 29	90
89.19%	sub_440180	0x440180	6 / 9	165 / 185	559
88.10%	sub_43651A	0x43651A	3 / 6	37 / 42	126
80.49%	sub_43496D	0x43496D	7 / 10	66 / 82	241
78.05%	sub_42D14D	0x42D14D	5 / 8	32 / 41	134
70.59%	sub_436598	0x436598	7 / 11	36 / 51	172
65.49%	sub_42CFD6	0x42CFD6	6 / 9	74 / 113	375
62.50%	sub_435C64	0x435C64	4 / 7	20 / 32	93
47.44%	sub_43B510	0x43B510	6 / 21	74 / 156	504
46.55%	sub_43BEFB	0x43BEFB	4 / 21	27 / 58	221
45.62%	sub_43573D	0x43573D	14 / 29	73 / 160	493
34.06%	sub_42B605	0x42B605	7 / 17	47 / 138	449
26.43%	sub_4337FB	0x4337FB	10 / 45	74 / 280	1019
19.23%	sub_42DAFB	0x42DAFB	2 / 5	10 / 52	145

Radio de cobertura.



Ruta al método IPersistStorage::Load.

ENCONTRAR LA VULNERABILIDAD

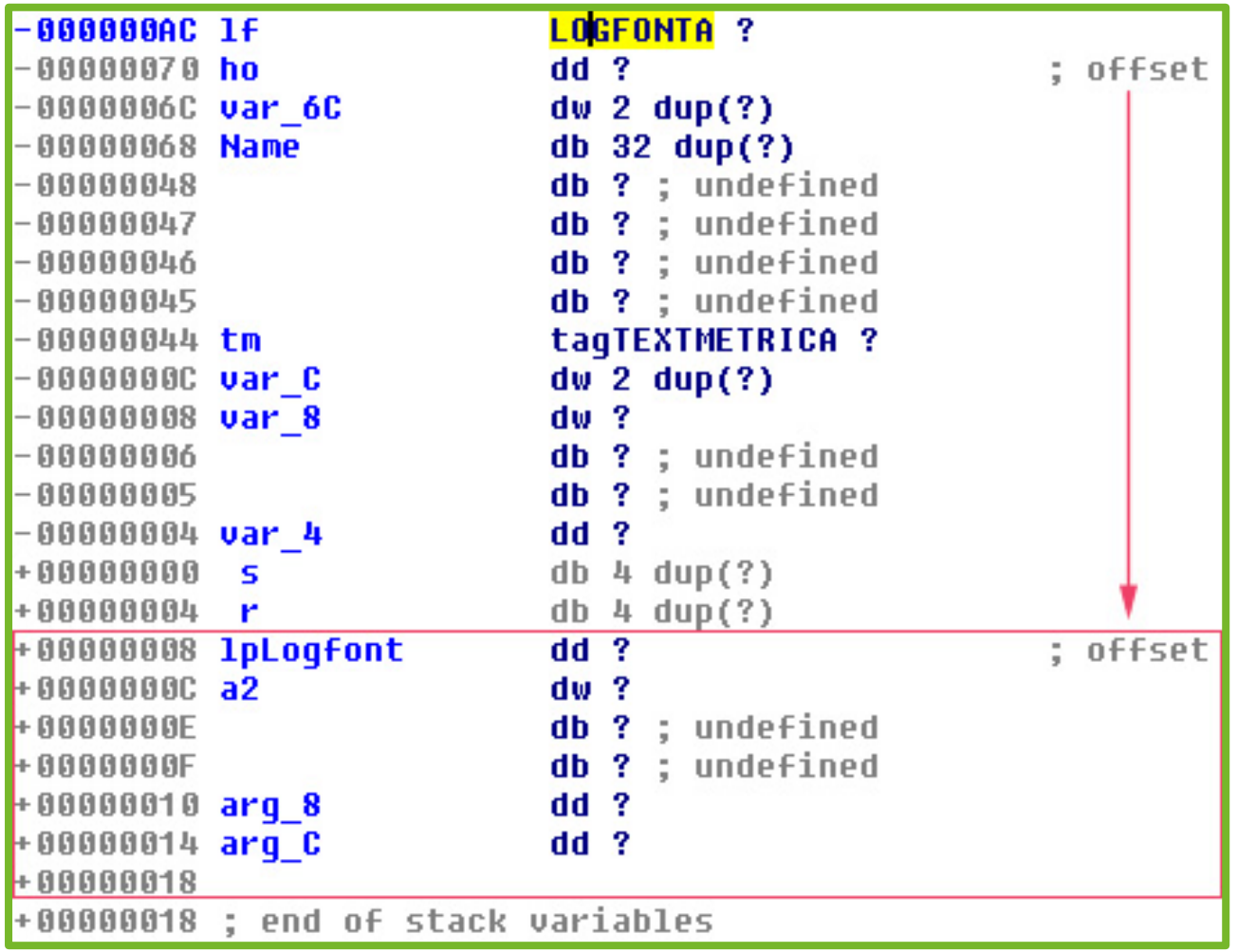
Encontrar la vulnerabilidad

- Una opción más clásica utilizada en el alcance de la investigación fue un desbordamiento basado en pila.
- La función con la dirección 004164FA fue la primera en llamarles la atención.

```
1  char *__cdecl get_null_term_string_from_formula_mem_descriptor(char *a1)
2  {
3    char *v1; // ST0C_4@1
4    char *result; // eax@2
5
6    do
7    {
8      v1 = a1++;
9      *v1 = inc_and_get_byte_from_counter_offset();
10   }
11   while ( *v1 );
12   result = a1;
13   *a1 = 0;
14   return result;
15 }
```

Encontrar la vulnerabilidad

- El procedimiento podría llamarse desde otros dos procedimientos, ambos procedimientos eran vulnerables al desbordamiento del búfer.
- Función tenía la dirección 00421774 y desbordaba un búfer en la estructura LOGFONTA.



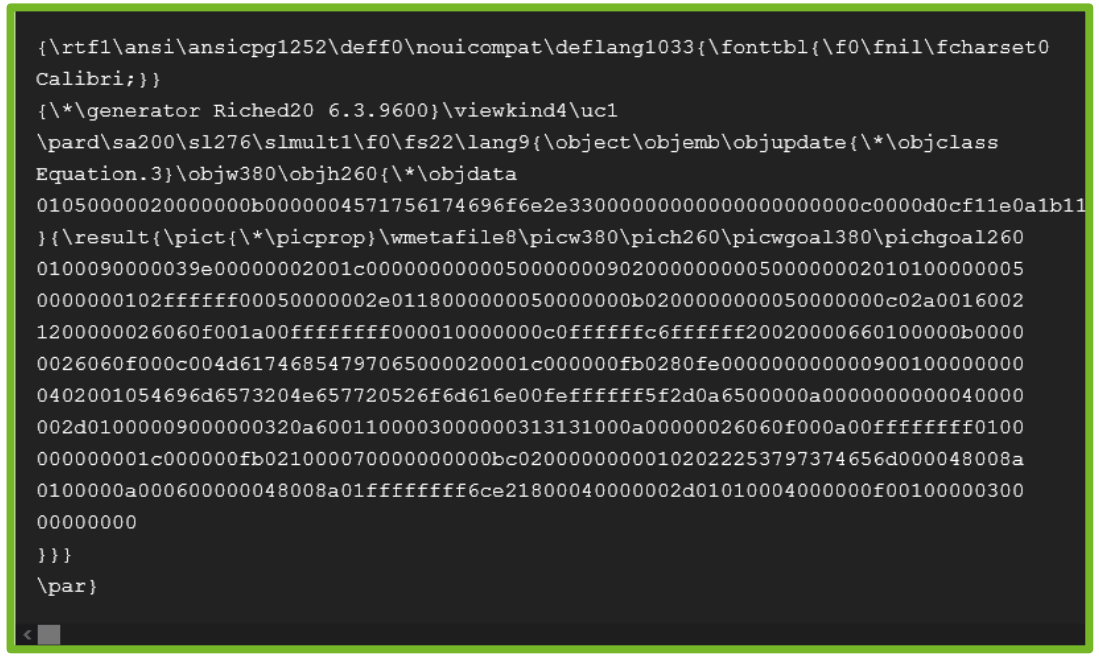
EXPLOTACIÓN DE VULNERABILIDADES

Explotación de vulnerabilidades

```
1  int __cdecl final_overflow(char *a1, char *a2, char *a3)
2  {
3    int result; // eax@12
4    char v4[36]; // [esp+Ch] [ebp-88h]@5
5    char v5[40]; // [esp+30h] [ebp-64h]@4
6    char *v6; // [esp+58h] [ebp-3Ch]@7
7    int v7; // [esp+5Ch] [ebp-38h]@1
8    __int16 v8; // [esp+60h] [ebp-34h]@1
9    int v9; // [esp+64h] [ebp-30h]@1
10   __int16 v10; // [esp+68h] [ebp-2Ch]@1
11   char overflow_buffer[36]; // [esp+6Ch] [ebp-28h]@1
12   int v12; // [esp+90h] [ebp-4h]@1
13
14   LOWORD(v12) = -1;
15   LOWORD(v7) = -1;
16   v8 = strlen(a1);
17   strcpy(overflow_buffer, a1);
18   _strupr(overflow_buffer);
19   v10 = sub_420FA0();
20   LOWORD(v9) = 0;
21   while ( v10 > (signed __int16)v9 )
22   {
23     if ( sub_420FBB(v9, v5) )
24     {
25       strcpy(v4, v5);
26       if ( *(signed __int16 *)&v5[33] == 1 )
27         _strupr(v4);
28       v6 = strstr(v4, a1);
29       if ( v6 || (v6 = strstr(v4, overflow_buffer)) != 0 )
30       {
31         if ( !a2 || !strstr(v4, a2) )
32         {
33           if ( (signed __int16)strlen(v5) == v8 )
34           {
35             strcpy(a3, v5);
36             return 1;
37           }
```

Explotación de vulnerabilidades

- Al insertar varios OLE que explotaban la vulnerabilidad descrita, fue posible ejecutar una secuencia arbitraria de comandos
- Un atacante podría usar la actualización automática OLE, una de las características, estándar del procesador RTF en Microsoft Office. vulnerabilidad se activaría sin la interacción del usuario.



Explotación de vulnerabilidades

- *Exploit* creado:
  - Funciona con todas las versiones de Microsoft Office lanzadas en los últimos 17 años (incluido Microsoft Office 365).
  - Funciona con todas las versiones de Microsoft Windows (incluida Microsoft Windows 10 Creators Update).
  - Relevante para todo tipo de arquitecturas.
  - No interrumpe el trabajo de un usuario con Microsoft Office.
  - Si se abre un documento, no requiere ninguna interacción con un usuario.

RECOMENDACIONES SOBRE MEJORAS DE SEGURIDAD

Recomendaciones sobre mejoras de seguridad

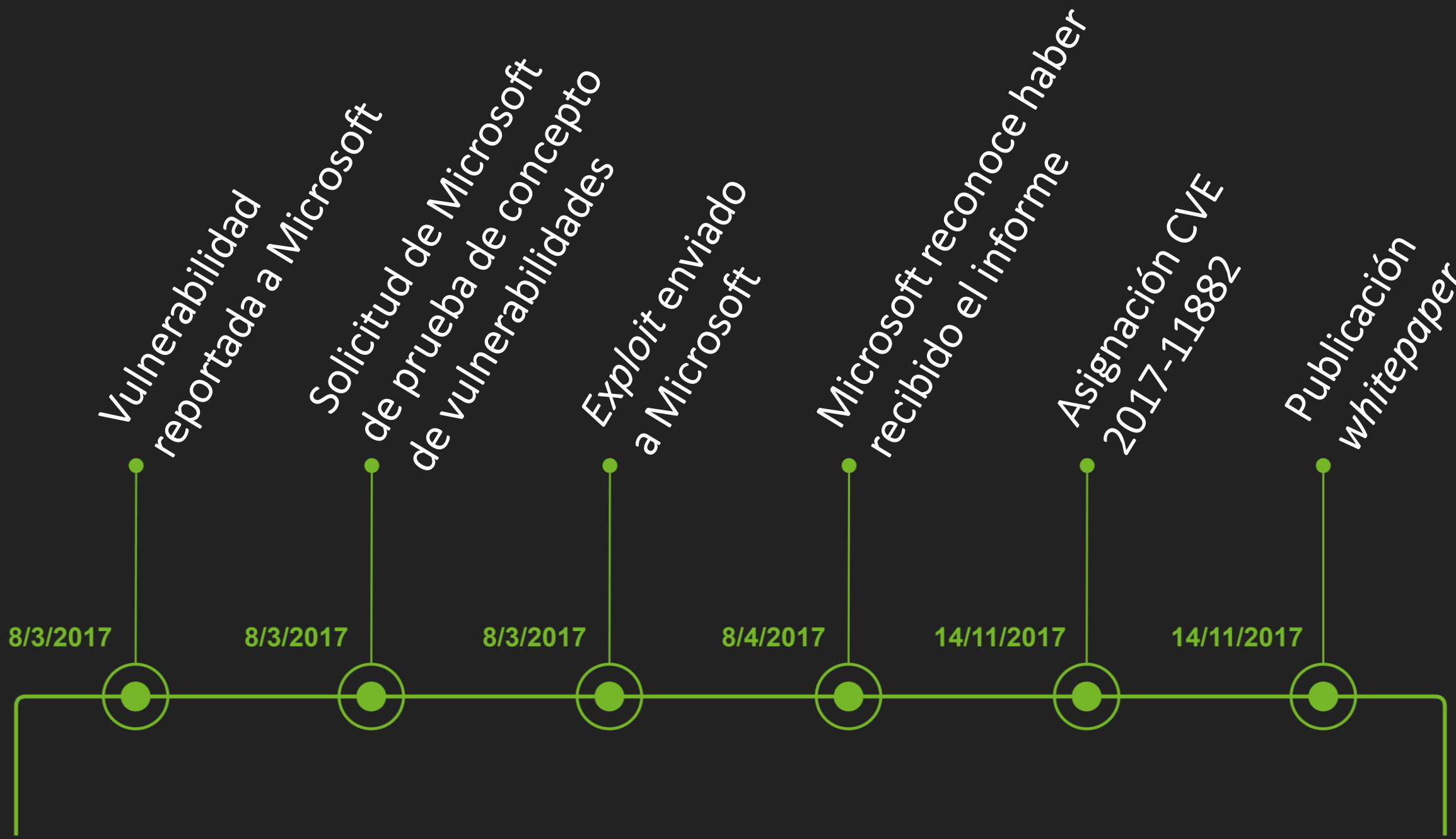
- La mejor opción para que un usuario garantice la seguridad es deshabilitar el registro del componente en el registro de Windows.

```
reg add "HKLM\SOFTWARE\Microsoft\Office\XX.X\Common\COM Compatibility\
{0002CE02-0000- 0000-C000-000000000046}" /v "Compatibility Flags" /t REG_DWORD /d
0x400

reg add "HKLM\SOFTWARE\Wow6432Node\Microsoft\Office\XX.X\Common\COM Compatibility\
{0002CE02-0000-0000-C000-000000000046}" /v "Compatibility Flags" /t REG_DWORD /d
0x400
```

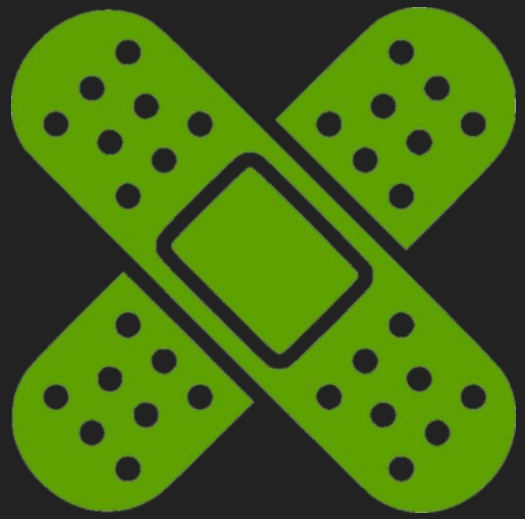
- El sandbox de Microsoft Office (Vista protegida) está bien diseñado, reduce la superficie de ataque al prohibir la ejecución y actualización de contenido activo (OLE / ActiveX / Macro).

DISCLOSURE TIMELINE


Vulnerabilidad reportada a Microsoft
8/3/2017
Solicitud de Microsoft de prueba de concepto de vulnerabilidades
8/3/2017
Exploit enviado a Microsoft
8/3/2017
Microsoft reconoce haber recibido el informe
8/4/2017
Asignación CVE 2017-11882
14/11/2017
Publicación whitepaper
14/11/2017

MICROPATCHING

Micropatching



PATCH

https://blog.0patch.com/2017/11/did-microsoft-just-manually-patch-their.html (17/11/2017)

https://blog.0patch.com/2017/11/official-patch-for-cve-2017-11882-meets.html (23/11/2017)

IMPACTO

Impacto

De hecho, CVE-2017-11882 es una de las vulnerabilidades más explotadas, e incluso llegó a la lista Recorded Future dedicada a las 10 vulnerabilidades más explotadas en 2018.

CVE-2017-11882 : Exploit que ataca sistemas con Microsoft Office sin parchear, como Word, Excel y PowerPoint.

Grupo de piratería Cobalt también utilizó esta falla de seguridad como arma en una de sus campañas a fines de noviembre (DDL Colbalt Strike)

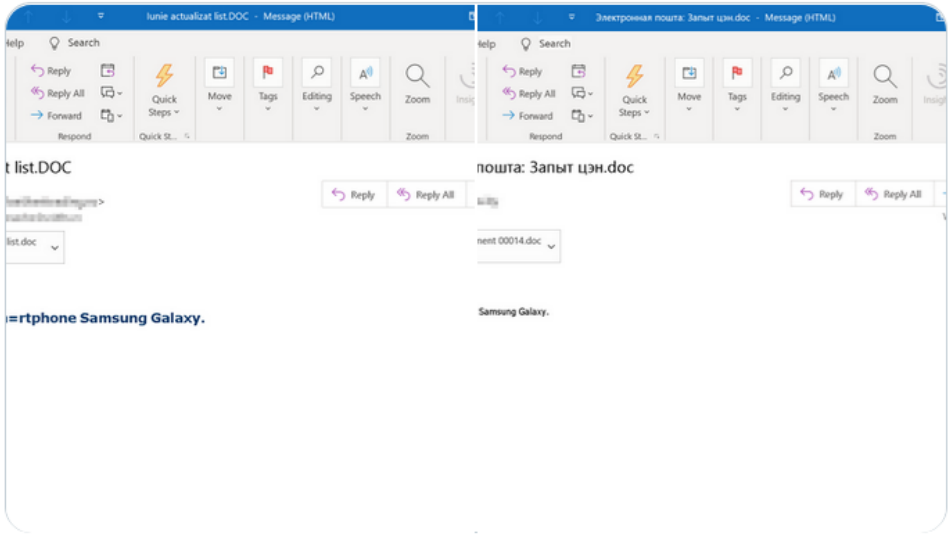
Un informe del FBI publicado el 12 de mayo de 2020 lo enumeró como una de las 10 principales vulnerabilidades que se explotan habitualmente

https://www.fortinet.com/blog/threat-research/new-remcos-rat-variant-is-spreading-by-exploiting-cve-2017-11882

Microsoft Security Intelligence ✓
@MsftSecIntel

Una campaña activa de malware que utiliza correos electrónicos en idiomas europeos distribuye archivos RTF que llevan el exploit CVE-2017-11882, que permite a los atacantes ejecutar automáticamente código malicioso sin requerir la interacción del usuario.

Traducir Tweet



12:07 a. m. · 8 jun. 2019 · Twitter Web Client

169 Retweets **25** Tweets citados **343** Me gusta

https://twitter.com/MsftSecIntel/status/1137118977983897600

Seguridad

El FBI revela las 10 vulnerabilidades más explotadas en 2020

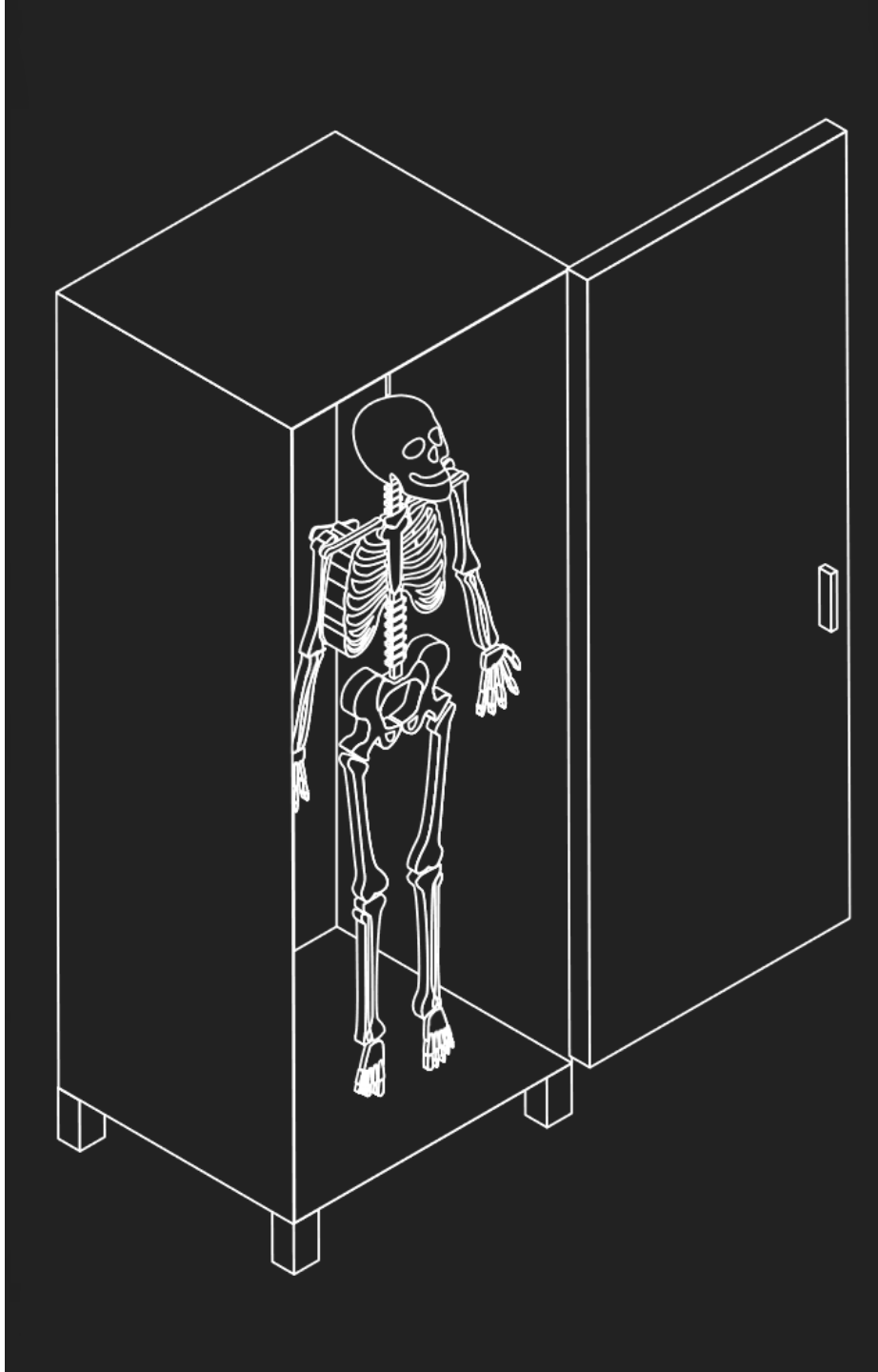
Alberto García | Publicado el 18 de mayo, 2020 • 20:00

https://www.adslzone.net/noticias/seguridad/vulnerabilidades-mas-explotadas-2020/

CONCLUSIÓN

Conclusión

- Incluso SDL no puede evitar que surjan vulnerabilidades que se explotan fácilmente.
- El código heredado y de terceros es una fuente de gran preocupación para un proveedor.
- La mitigación de la seguridad tiene una importancia vital, considerando las realidades del mundo moderno.
- El software y los sistemas, en general, deben actualizarse y recibir soporte.



Referencias

- https://web.archive.org/web/20180811110001/https://embedi.com/blog/skeleton-closet-ms-office-vulnerability-you-didnt-know-about/
- https://web.archive.org/web/20180510111801/https://embedi.com/wp-content/uploads/dlm_uploads/2017/11/skeleton-in-the-closet.pdf
- https://github.com/embedi/CVE-2017-11882
- https://www.wsg127.com/vulnerabilidad-microsoft/
- https://fwhibbit.es/explotando-vulnerabilidades-cve-2017-11882
- https://blog.0patch.com/2017/11/did-microsoft-just-manually-patch-their.html
- https://blog.0patch.com/2017/11/official-patch-for-cve-2017-11882-meets.html
- https://blog.reversinglabs.com/blog/reversinglabs-yara-rule-detects-cobalt-payload-exploiting-cve-2017-11882

Referencias

- https://nakedsecurity.sophos.com/2019/06/10/microsoft-warns-of-time-travelling-equation-exploit-are-you-safe/
- https://www.codeproject.com/Questions/394365/what-is-inproc-and-outproc
- https://blog.satinfo.es/2019/cve-2017-11882-exploit-que-ataca-sistemas-con-microsoft-office-sin-parchear-como-word-excel-y-powerpoint/
- 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.menlosecurity.com/blog/equation-editor-attackers-continue-to-exploit-cve-2017-1182
- https://www.fortinet.com/blog/threat-research/new-remcos-rat-variant-is-spreading-by-exploiting-cve-2017-11882

Referencias

- https://sensorstechforum.com/cve-2017-11882-european-email-attacks/
- https://threatpost.com/microsoft-arbitrary-code-execution-old-bug/145527/
- https://www.techradar.com/news/this-microsoft-office-exploit-was-patched-years-ago-but-is-still-being-abused-by-hackers
- https://www.techradar.com/news/hackers-have-revived-a-decade-old-microsoft-office-exploit-and-theyre-having-a-field-day
- https://www.key4biz.it/lodarat-il-trojan-bancario-affina-lo-spying-e-diventa-multipiattaforma/344584/
- https://www.expresscomputer.in/security/agent-tesla-malware-exploiting-ms-office-vulnerabilities-report/54464/
- https://www.channelpartner.es/seguridad/noticias/1115043002502/campanas-de-malware-se-ceban-usuarios-espanoles-octubre.1.html

FIN

Presentación basada en:

Skeleton in the closet, MS Office vulnerability you didn’t know about (2017)