FIRST GÉANT

MARCH 2-3, 2022
VIRTUAL SYMPOSIUM FOR EUROPE
& JOINT TF-CSIRT MEETING

Fuzzing Windows Media Foundation in 2021

Milan Kyselica (IstroCSIRT)

$WHOAMI

- Penetration tester -> Head of Offensive Security Department
- Experience with Web/Infra/Cloud PT, Red Teaming, Social Engineering and Attack Simulation
- Web application security research
- Various fuzzing projects (OS, PDF readers, Browsers, V8 and others…)
- GCPN, OSCP, OSWP, CRTP, CRTE …

FUZZING !?

- Still relevant
- Different approaches

Flow of fuzzing

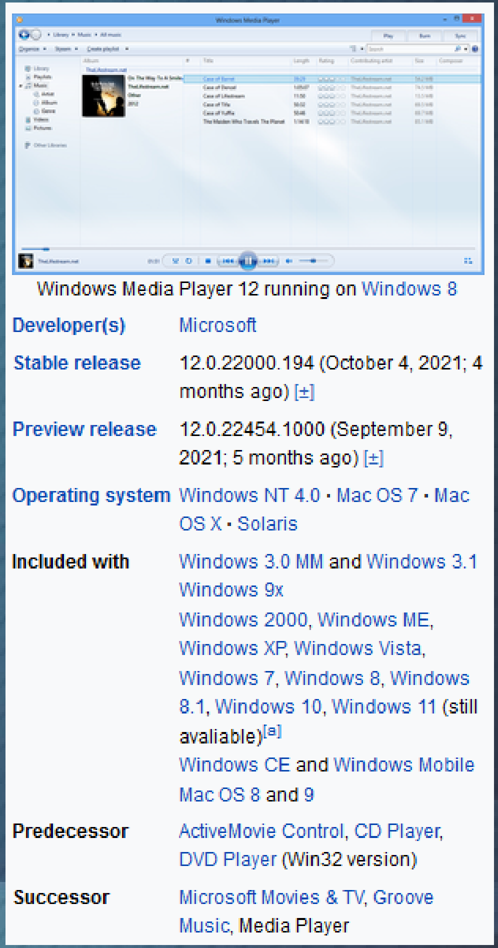
1. Create a corpus (test cases)
2. Take the file and modify it (mutation)
3. Run program with the 'new' file

Fuzzing the application as is
Fuzzing the application with a harness
imgflip.com

Credit - https://bishopfox.com/blog/fuzzing-aka-fuzz-testing

Windows Media Player

- Default media player in Windows (up to Windows 11)
- A lot of features (bigger attack surface)
- Can play a range of file formats
- 32&64bit

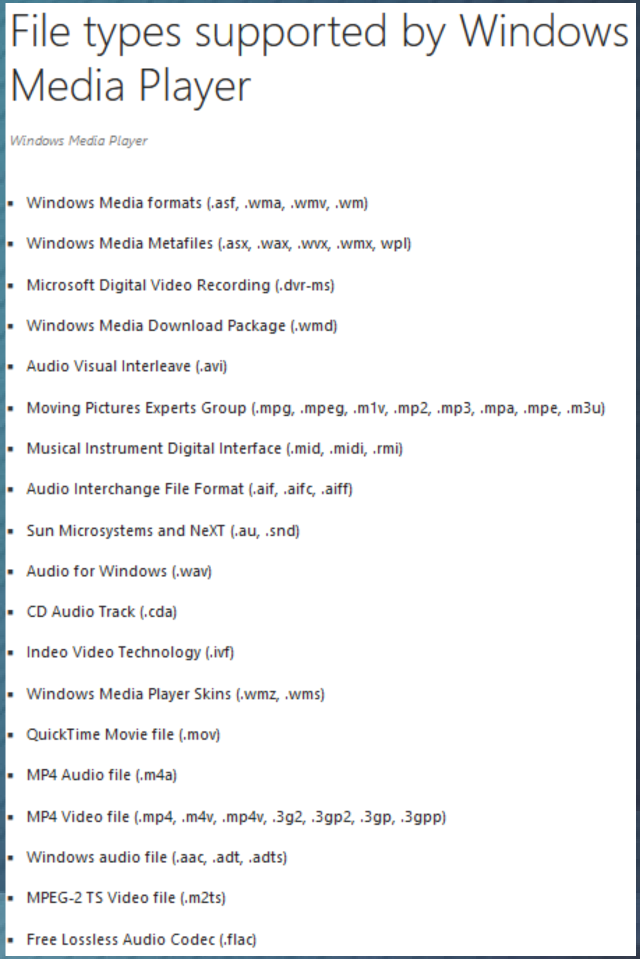


Windows Media Player 12 running on Windows 8

Developer(s)	Microsoft
Stable release	12.0.22000.194 (October 4, 2021; 4 months ago) [±]
Preview release	12.0.22454.1000 (September 9, 2021; 5 months ago) [±]
Operating system	Windows NT 4.0 · Mac OS 7 · Mac OS X · Solaris
Included with	Windows 3.0 MM and Windows 3.1 Windows 9x Windows 2000, Windows ME, Windows XP, Windows Vista, Windows 7, Windows 8, Windows 8.1, Windows 10, Windows 11 (still available)[a] Windows CE and Windows Mobile Mac OS 8 and 9
Predecessor	ActiveMovie Control, CD Player, DVD Player (Win32 version)
Successor	Microsoft Movies & TV, Groove Music, Media Player

File Format

- Support documents (support.microsoft.com)
- Undocumented file formats ???
- Latest media file types supported elsewhere
- File structure & complexity
- RE -> functions and DLLs



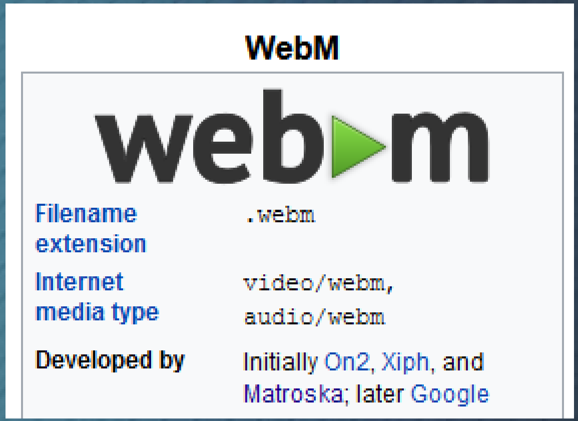
File types supported by Windows Media Player

Windows Media Player

- Windows Media formats (.asf, .wma, .wmv, .wm)
- Windows Media Metafiles (.asx, .wax, .wvx, .wmx, wpl)
- Microsoft Digital Video Recording (.dvr-ms)
- Windows Media Download Package (.wmd)
- Audio Visual Interleave (.avi)
- Moving Pictures Experts Group (.mpg, .mpeg, .m1v, .mp2, .mp3, .mpa, .mpe, .m3u)
- Musical Instrument Digital Interface (.mid, .midi, .rmi)
- Audio Interchange File Format (.aif, .aifc, .aiff)
- Sun Microsystems and NeXT (.au, .snd)
- Audio for Windows (.wav)
- CD Audio Track (.cda)
- Indeo Video Technology (.ivf)
- Windows Media Player Skins (.wmz, .wms)
- QuickTime Movie file (.mov)
- MP4 Audio file (.m4a)
- MP4 Video file (.mp4, .m4v, .mp4v, .3g2, .3gp2, .3gp, .3gpp)
- Windows audio file (.aac, .adt, .adts)
- MPEG-2 TS Video file (.m2ts)
- Free Lossless Audio Codec (.flac)

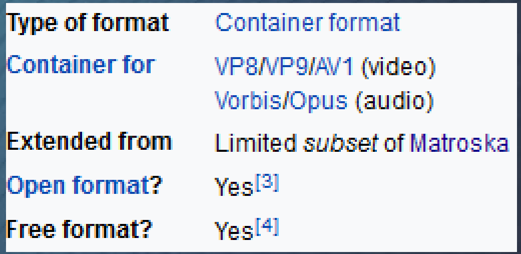
WebM file format

- Missing in the list of supported file types
- VP8, VP9, AV1 & Vorbis, Opus
- Understanding valid .webm file
- Which functions are being used ?
- Code coverage increase ?
- Let's try to play it…



WebM

Filename extension	`.webm`
Internet media type	`video/webm`, `audio/webm`
Developed by	Initially On2, Xiph, and Matroska; later Google



Type of format	Container format
Container for	VP8/VP9/AV1 (video) Vorbis/Opus (audio)
Extended from	Limited *subset* of Matroska
Open format?	Yes[3]
Free format?	Yes[4]

Let’s FUZZ

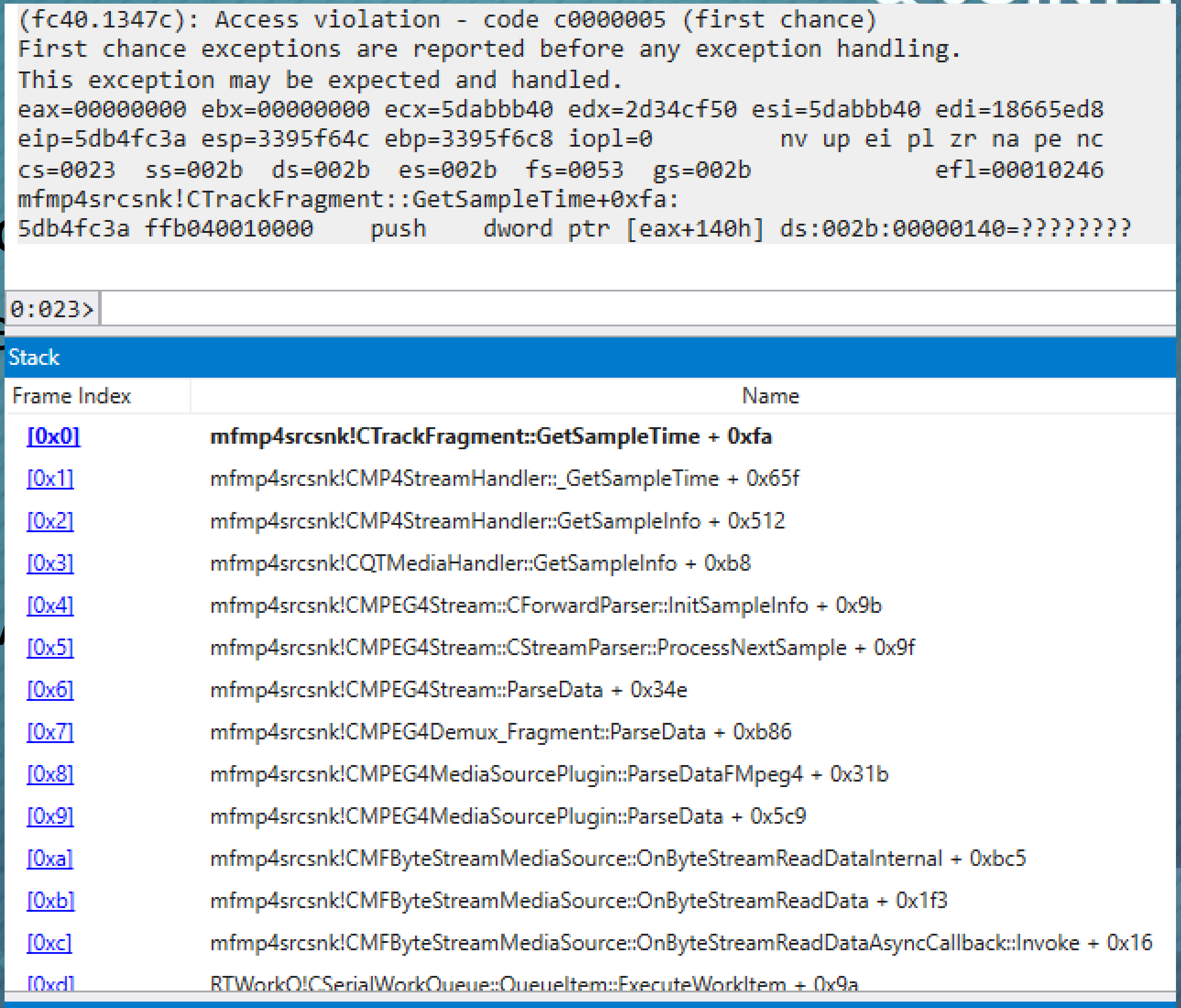
1. Build a VM only for fuzzing (focus on performance)
2. Corpus preparation (based on file type)
3. File mutation setting (can be difficult)
4. Execute the target program with a modified input file
5. If everything works, execute the fuzzing script

Crash triage

- Manual/Auto
- What are we

Tools

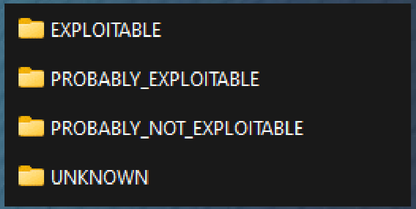
- Windbg Prev
- BugId
- !Exploitable



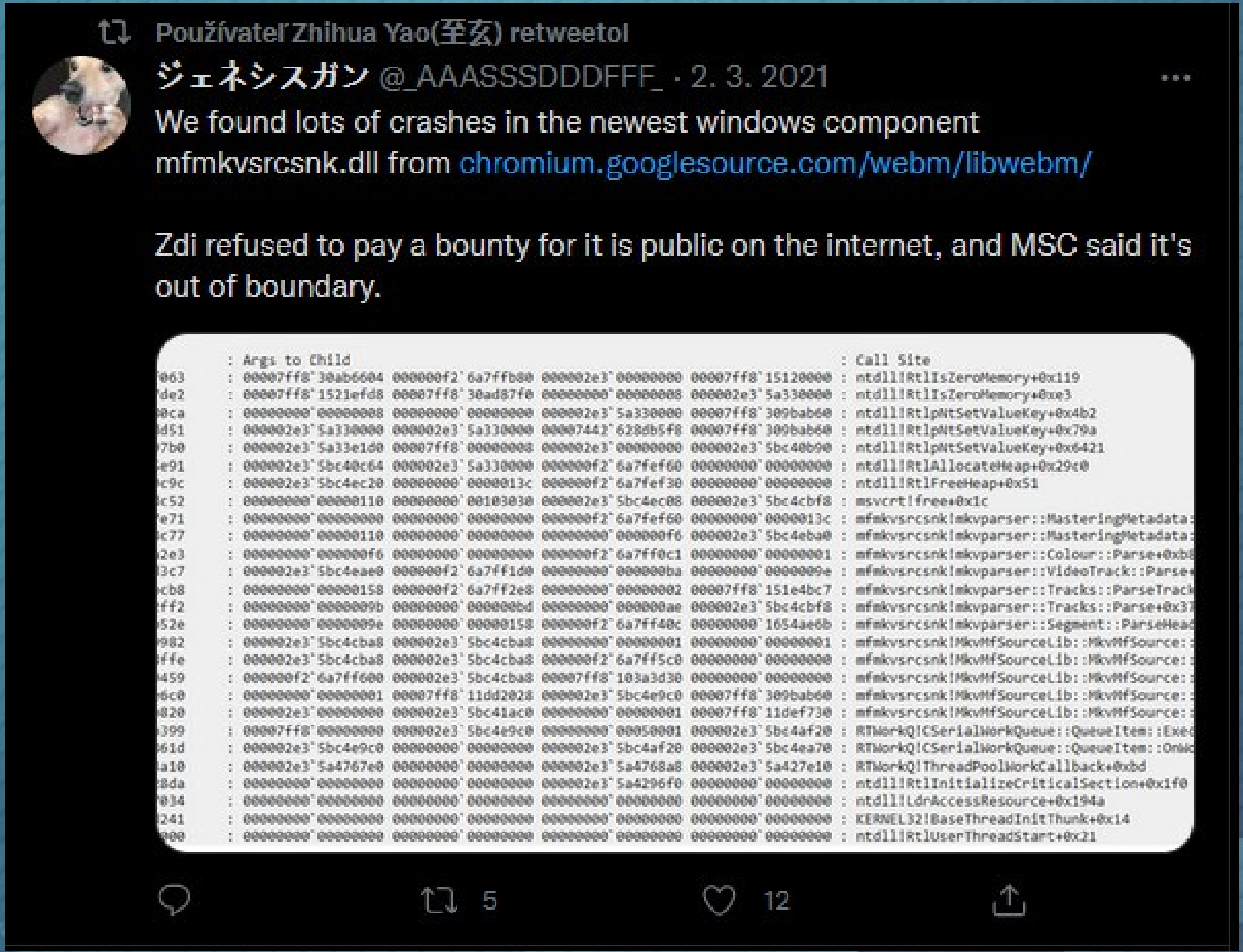
```
(fc40.1347c): Access violation - code c0000005 (first chance)
First chance exceptions are reported before any exception handling.
This exception may be expected and handled.
eax=00000000 ebx=00000000 ecx=5dabbb40 edx=2d34cf50 esi=5dabbb40 edi=18665ed8
eip=5db4fc3a esp=3395f64c ebp=3395f6c8 iopl=0         nv up ei pl zr na pe nc
cs=0023  ss=002b  ds=002b  es=002b  fs=0053  gs=002b             efl=00010246
mfmp4srcsnk!CTrackFragment::GetSampleTime+0xfa:
5db4fc3a ffb040010000    push    dword ptr [eax+140h] ds:002b:00000140=????????

0:023>
```

Stack

Frame Index	Name
[0x0]	**mfmp4srcsnk!CTrackFragment::GetSampleTime + 0xfa**
[0x1]	mfmp4srcsnk!CMP4StreamHandler::_GetSampleTime + 0x65f
[0x2]	mfmp4srcsnk!CMP4StreamHandler::GetSampleInfo + 0x512
[0x3]	mfmp4srcsnk!CQTMediaHandler::GetSampleInfo + 0xb8
[0x4]	mfmp4srcsnk!CMPEG4Stream::CForwardParser::InitSampleInfo + 0x9b
[0x5]	mfmp4srcsnk!CMPEG4Stream::CStreamParser::ProcessNextSample + 0x9f
[0x6]	mfmp4srcsnk!CMPEG4Stream::ParseData + 0x34e
[0x7]	mfmp4srcsnk!CMPEG4Demux_Fragment::ParseData + 0xb86
[0x8]	mfmp4srcsnk!CMPEG4MediaSourcePlugin::ParseDataFMpeg4 + 0x31b
[0x9]	mfmp4srcsnk!CMPEG4MediaSourcePlugin::ParseData + 0x5c9
[0xa]	mfmp4srcsnk!CMFByteStreamMediaSource::OnByteStreamReadDataInternal + 0xbc5
[0xb]	mfmp4srcsnk!CMFByteStreamMediaSource::OnByteStreamReadData + 0x1f3
[0xc]	mfmp4srcsnk!CMFByteStreamMediaSource::OnByteStreamReadDataAsyncCallback::Invoke + 0x16
[0xd]	RTWorkQ!CSerialWorkQueue::QueueItem::ExecuteWorkItem + 0x9a



EXPLOITABLE
PROBABLY_EXPLOITABLE
PROBABLY_NOT_EXPLOITABLE
UNKNOWN



Používateľ Zhihua Yao(至玄) retweetol

ジェネシスガン @_AAASSSDDDFFF_ · 2. 3. 2021

We found lots of crashes in the newest windows component mfmkvsrcsnk.dll from chromium.googlesource.com/webm/libwebm/

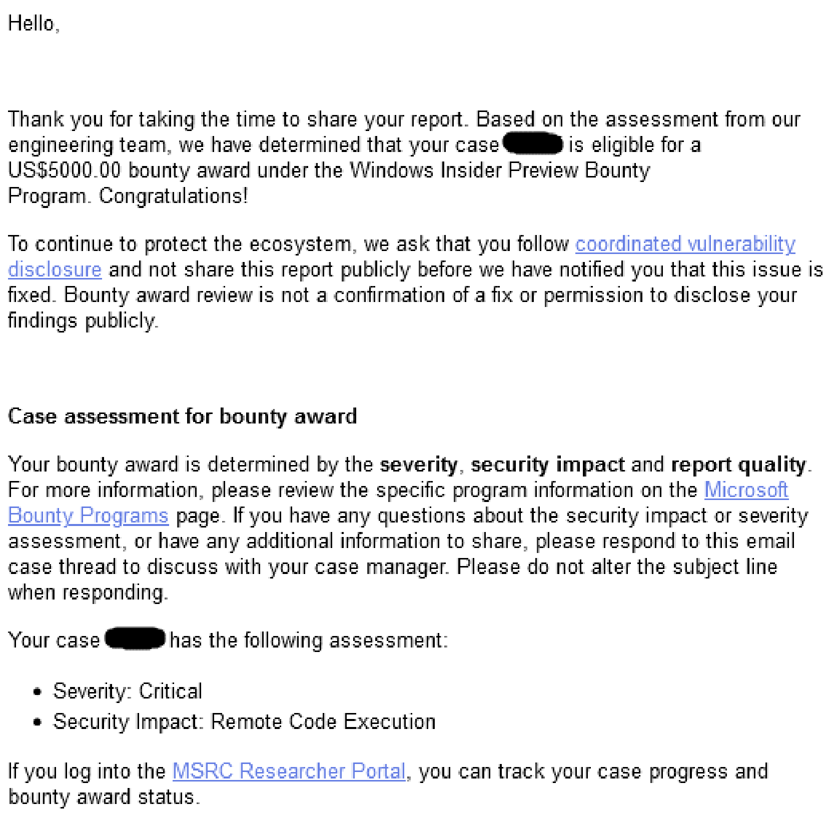
Zdi refused to pay a bounty for it is public on the internet, and MSC said it's out of boundary.

```
        : Args to Child                                                                 : Call Site
f063    : 00007ff8`30ab6604 000000f2`6a7ffb80 000002e3`00000000 00007ff8`15120000 : ntdll!RtlIsZeroMemory+0x119
de2     : 00007ff8`1521efd8 00007ff8`30ad87f0 00000000`00000008 000002e3`5a330000 : ntdll!RtlIsZeroMemory+0xe3
0ca     : 00000000`00000008 00000000`00000000 000002e3`5a330000 00007ff8`309bab60 : ntdll!RtlpNtSetValueKey+0x4b2
d51     : 000002e3`5a330000 000002e3`5a330000 00007442`628db5f8 00007ff8`309bab60 : ntdll!RtlpNtSetValueKey+0x79a
7b0     : 000002e3`5a33e1d0 00007ff8`00000008 000002e3`00000000 000002e3`5bc40b90 : ntdll!RtlpNtSetValueKey+0x6421
e91     : 000002e3`5bc40c64 000002e3`5a330000 000000f2`6a7fef60 00000000`00000000 : ntdll!RtlAllocateHeap+0x29c0
c9c     : 000002e3`5bc4ec20 00000000`0000013c 000000f2`6a7fef30 00000000`00000000 : ntdll!RtlFreeHeap+0x51
c52     : 00000000`00000110 00000000`00103030 000002e3`5bc4ec08 000002e3`5bc4cbf8 : msvcrt!free+0x1c
e71     : 00000000`00000000 00000000`00000000 000000f2`6a7fef60 00000000`0000013c : mfmkvsrcsnk!mkvparser::MasteringMetadata:
c77     : 00000000`00000110 00000000`00000000 00000000`000000f6 000002e3`5bc4eba0 : mfmkvsrcsnk!mkvparser::MasteringMetadata:
2e3     : 00000000`000000f6 00000000`00000000 000000f2`6a7ff0c1 00000000`00000001 : mfmkvsrcsnk!mkvparser::Colour::Parse+0xb
3c7     : 000002e3`5bc4eae0 000000f2`6a7ff1d0 00000000`000000ba 00000000`0000009e : mfmkvsrcsnk!mkvparser::VideoTrack::Parse
cb8     : 00000000`00000158 000000f2`6a7ff2e8 00000000`00000002 00007ff8`151e4bc7 : mfmkvsrcsnk!mkvparser::Tracks::ParseTrack
ff2     : 00000000`0000000b 00000000`000000bd 00000000`000000ae 000002e3`5bc4cbf8 : mfmkvsrcsnk!mkvparser::Tracks::Parse+0x3
52e     : 00000000`0000009e 00000000`00000158 000000f2`6a7ff40c 00000000`1654ae6b : mfmkvsrcsnk!mkvparser::Segment::ParseHead
982     : 000002e3`5bc4cba8 000002e3`5bc4cba8 00000000`00000001 00000000`00000001 : mfmkvsrcsnk!MkvMfSourceLib::MkvMfSource::
ffe     : 000002e3`5bc4cba8 000002e3`5bc4cba8 000000f2`6a7ff5c0 00000000`00000000 : mfmkvsrcsnk!MkvMfSourceLib::MkvMfSource::
459     : 000000f2`6a7ff600 000002e3`5bc4cba8 00007ff8`103a3d30 00000000`00000000 : mfmkvsrcsnk!MkvMfSourceLib::MkvMfSource::
6c0     : 00000000`00000001 00007ff8`11dd2028 000002e3`5bc4e9c0 00007ff8`309bab60 : mfmkvsrcsnk!MkvMfSourceLib::MkvMfSource::
820     : 000002e3`00000000 000002e3`5bc41ac0 00000000`00000001 00007ff8`11def730 : mfmkvsrcsnk!MkvMfSourceLib::MkvMfSource::
399     : 00007ff8`00000000 000002e3`5bc4e9c0 00000000`00050001 000002e3`5bc4af20 : RTWorkQ!CSerialWorkQueue::QueueItem::Exec
61d     : 000002e3`5bc4e9c0 00000000`00000000 000002e3`5bc4af20 000002e3`5bc4ea70 : RTWorkQ!CSerialWorkQueue::QueueItem::OnW
a10     : 000002e3`5a4767e0 00000000`00000000 000002e3`5a4768a8 000002e3`5a427e10 : RTWorkQ!ThreadPoolWorkCallback+0xbd
8da     : 00000000`00000000 00000000`00000000 000002e3`5a4296f0 00000000`00000000 : ntdll!RtlInitializeCriticalSection+0x1f0
034     : 00000000`00000000 00000000`00000000 00000000`00000000 00000000`00000000 : ntdll!LdrAccessResource+0x194a
241     : 00000000`00000000 00000000`00000000 00000000`00000000 00000000`00000000 : KERNEL32!BaseThreadInitThunk+0x14
000     : 00000000`00000000 00000000`00000000 00000000`00000000 00000000`00000000 : ntdll!RtlUserThreadStart+0x21
```

5 12

RESULTS

- 6 months of 24/7 fuzzing on multiple VMs
- 10 000+ crashes (>99% not exploitable)
- 23 unique, a lot of Read AV, NULL Dereference…
- 2x Critical Remote Code Execution vulnerability
- 2x Patch Tuesday CVE-2021-41330 & CVE-2022-XXXXX



Hello,

Thank you for taking the time to share your report. Based on the assessment from our engineering team, we have determined that your case [redacted] is eligible for a US$5000.00 bounty award under the Windows Insider Preview Bounty Program. Congratulations!

To continue to protect the ecosystem, we ask that you follow coordinated vulnerability disclosure and not share this report publicly before we have notified you that this issue is fixed. Bounty award review is not a confirmation of a fix or permission to disclose your findings publicly.

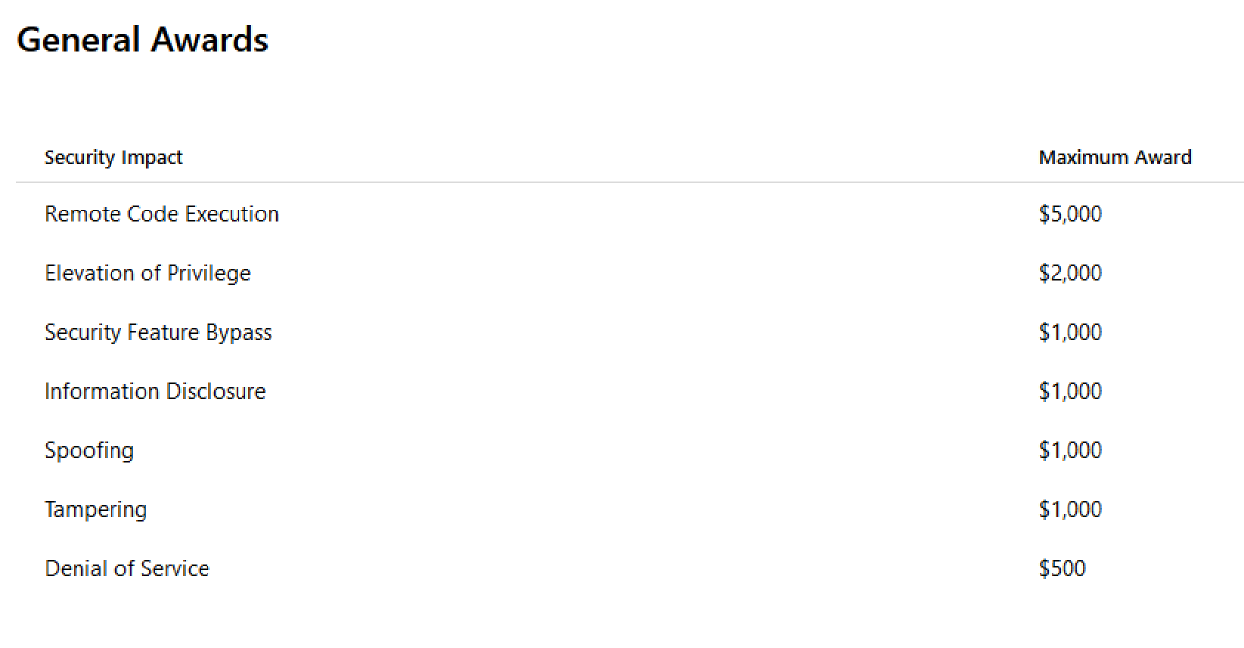
Case assessment for bounty award

Your bounty award is determined by the **severity**, **security impact** and **report quality**. For more information, please review the specific program information on the Microsoft Bounty Programs page. If you have any questions about the security impact or severity assessment, or have any additional information to share, please respond to this email case thread to discuss with your case manager. Please do not alter the subject line when responding.

Your case [redacted] has the following assessment:

- Severity: Critical
- Security Impact: Remote Code Execution

If you log into the MSRC Researcher Portal, you can track your case progress and bounty award status.



General Awards

Security Impact	Maximum Award
Remote Code Execution	$5,000
Elevation of Privilege	$2,000
Security Feature Bypass	$1,000
Information Disclosure	$1,000
Spoofing	$1,000
Tampering	$1,000
Denial of Service	$500

Lessons Learned

- You have to be fast (otherwise it will be a duplicate ☺)
- It still does make sense to fuzz
- Be creative and create your own fuzzing environment
- There is always a place for optimalization (PCIe 4.0 4x, RAM, Harnesses, program patching…)
- Be patient, it takes **a lot of time**

Thanks for watching !