# Flexera FlexNet Publisher lmadmin Message 282 Remote DoS

Medium

← View More Research Advisories

## Synopsis

The flaw exists in lmadmin due to improper validation of user-supplied data when processing a FLEX_MSG_QUORUM message. An unauthenticated, remote attacker can specify a large, signed 32-bit integer (i.e., 0x7fffffff) in the message to cause the C++ new operator to throw an unhandled exception, resulting in process termination:

```
.text:005012B3           lea     eax, [ebp+int32] ; attacker-controlled; ie: 0x7fffffff
.text:005012B6           push    eax
.text:005012B7           mov     ecx, [ebp+pos]
.text:005012BA           push    ecx
.text:005012BB           mov     edx, [ebp+arg_sebuf]
.text:005012BE           push    edx
.text:005012BF           mov     ecx, [ebp+var_28]
.text:005012C2           call    obj14_sebufGetBe32 ; return true/false
.text:005012C7           movzx   eax, al
.text:005012CA           test    eax, eax
.text:005012CC           jnz     short loc_5012D5
.text:005012CE           xor     al, al
.text:005012D0           jmp     loc_50139A
.text:005012D5 ; ---------------------------------------------------------------------------
.text:005012D5
.text:005012D5 loc_5012D5:                   ; CODE XREF: obj14_Parse_FLEX_MSG_QUORUM+5C↑j
.text:005012D5           mov     ecx, [ebp+pos]
.text:005012D8           add     ecx, 4
.text:005012DB           mov     [ebp+pos], ecx
.text:005012DE           mov     [ebp+var_18], 0
.text:005012E5           cmp     [ebp+int32], 0
.text:005012E9           jle     short negative_size
.text:005012EB           mov     edx, [ebp+int32] ; attacker-controlled
.text:005012EB                                ; 0x7fffffff -> unhandled exception
.text:005012EE           push    edx
.text:005012EF           call    ??_U@YAPAXI@Z ; operator new[](uint)
```

Unhandled exception in 32-bit lmadmin.exe (v11.16.5.1):

```
(1284.1488): C++ EH exception - code e06d7363 (first chance)
(1284.1488): C++ EH exception - code e06d7363 (!!! second chance !!!)
eax=09cffae0 ebx=08c70c40 ecx=00000003 edx=00000000 esi=03fecba8 edi=09cffb80
eip=7d85c5af esp=09cffae0 ebp=09cffb30 iopl=0         nv up ei pl nz ac po nc
cs=0023  ss=002b  ds=002b  es=002b  fs=0053  gs=002b             efl=00000212
KERNELBASE!RaiseException+0x58:
7d85c5af c9              leave
0:008> kb
ChildEBP RetAddr  Args to Child
09cffb30 03fd8a19 e06d7363 00000001 00000003 KERNELBASE!RaiseException+0x58
09cffb70 0401dea6 09cffb80 03fecba8 03fed3e4 MSVCR120!_CxxThrowException+0x5b [f:\dd\vctools\crt\crtw32\eh\throw.cpp @ 152]
09cffb90 005012f4 7fffffff 1e9495d9 0000000f MSVCR120!operator new+0x50 [f:\dd\vctools\crt\crtw32\heap\new.cpp @ 62]
WARNING: Stack unwind information not available. Following frames may be wrong.
09cffbd4 004f58a8 09cffdcc 09cffe48 1e9493b5 lmadmin!xalanc_1_11::XalanMemoryManager::operator=+0x5adf4
09cffdb8 004f46c6 09cffdcc 09cffe48 1e94906d lmadmin!xalanc_1_11::XalanMemoryManager::operator=+0x4f3a8
09cffe60 00536521 1e949081 0954fc04 00000000 lmadmin!xalanc_1_11::XalanMemoryManager::operator=+0x4e1c6
09cffe8c 00536de5 00000003 08c6cfe8 09cffeb0 lmadmin!xalanc_1_11::XalanMemoryManager::operator=+0x90021
09cffe9c 005365fd 0954fbd4 00000003 08c6cfec lmadmin!xalanc_1_11::XalanMemoryManager::operator=+0x908e5
09cffeb0 00536dc0 00000000 08c6cfe8 09cffecf lmadmin!xalanc_1_11::XalanMemoryManager::operator=+0x900fd
09cffed0 00537395 08c6cfe8 09cfff10 0042829b lmadmin!xalanc_1_11::XalanMemoryManager::operator=+0x908c0
09cffedc 0042829b 08c6cfe8 1e94911d 09cfff68 lmadmin!xalanc_1_11::XalanMemoryManager::operator=+0x90e95
09cfff10 004f28e2 08c6cfa0 09cfff44 00630cee lmadmin+0x2829b
09cfff1c 00630cee 1e949149 00000000 0b040c40 lmadmin!xalanc_1_11::XalanMemoryManager::operator=+0x4c3e2
09cfff44 03fec129 08c6cfa0 2e566c36 00000000 lmadmin!xalanc_1_11::XalanMemoryManager::operator=+0x18a7ee
09cfff7c 03fec10d 00000000 09cfff94 7dd7343d MSVCR120!_callthreadstartex+0x1b [f:\dd\vctools\crt\crtw32\startup\threadex.c @ 381]
09cfff88 7dd7343d 08c70c40 09cfffd4 7dea9812 MSVCR120!_threadstartex+0x69 [f:\dd\vctools\crt\crtw32\startup\threadex.c @ 359]
09cfff94 7dea9812 08c70c40 44e2d13e 00000000 kernel32!BaseThreadInitThunk+0xe
09cfffd4 7dea97e5 03fec0cc 08c70c40 ffffffff ntdll!__RtlUserThreadStart+0x70
09cfffec 00000000 03fec0cc 08c70c40 00000000 ntdll!_RtlUserThreadStart+0x1b
```

## Proof of Concept

flexera_fnp_lmadmin_msg_282_dos_cve-2020-12080.py

Attached is a PoC to terminate lmadmin.exe. The PoC can be used as follows:

```
python flexera_fnp_lmadmin_msg_282_dos_cve-2020-12080.py -t  -p 27000
```

## Solution

Upgrade to 11.17.0

## Additional References

https://community.flexera.com/t5/FlexNet-Publisher-Knowledge-Base/CVE-2020-12080-Remediated-in-FlexNet-Publisher/ta-p/143873/jump-to/first-unread-message
https://community.flexera.com/t5/FlexNet-Publisher-News/FlexNet-Publisher-2020-R2-11-17-0-is-here/ba-p/144017/jump-to/first-unread-message

01/23/2020 - Second attempt at communication.
01/23/2020 - Flexera's engineering team is taking a look. They will get back to us.
01/29/2020 - Flexera mentions 14-day extension clause in our policy and requests us "not to make this vulnerability public".
01/30/2020 - Tenable asks for clarification.
01/30/2020 - Flexera clarifies. They would like the 14 day extension only.
01/30/2020 - New disclosure date is set to April 28th.
02/26/2020 - Tenable follows up to ensure we are still on track for an April 28 release.
02/28/2020 - Flexera is still on track.
04/06/2020 - Tenable asks for an update.
04/06/2020 - Flexera is still projecting an April 28 release.
04/06/2020 - Tenable thanks Flexera.
04/23/2020 - Flexera expects to release on April 24. They will notify us when it's available to customers.
04/27/2020 - Tenable notices that a security bulletin was released on April 23. We will release our advisory today.

*All information within TRA advisories is provided "as is", without warranty of any kind, including the implied warranties of merchantability and fitness for a particular purpose, and with no guarantee of completeness, accuracy, or timeliness. Individuals and organizations are responsible for assessing the impact of any actual or potential security vulnerability.*

*Tenable takes product security very seriously. If you believe you have found a vulnerability in one of our products, we ask that you please work with us to quickly resolve it in order to protect customers. Tenable believes in responding quickly to such reports, maintaining communication with researchers, and providing a solution in short order.*

*For more details on submitting vulnerability information, please see our Vulnerability Reporting Guidelines page.*

*If you have questions or corrections about this advisory, please email advisories@tenable.com*

## Risk Information

**CVE ID:** CVE-2020-12080
**Tenable Advisory ID:** TRA-2020-28
**CVSSv2 Base / Temporal Score:** 7.8 / 6.1
**CVSSv2 Vector:** (AV:N/AC:L/Au:N/C:N/I:N/A:C)
**Affected Products:** FlexNet Publisher prior to 11.17.0
**Risk Factor:** Medium

## Advisory Timeline

04/27/2020 - Advisory published

**FEATURED PRODUCTS**

Tenable One Exposure Management Platform

Tenable.cs Cloud Security

Tenable.io Vulnerability Management

Tenable.io Web App Scanning

Tenable.asm External Attack Surface

Tenable.ad Active Directory

Tenable.ot Operational Technology

Tenable.sc Security Center

Tenable Lumin

Nessus

→ View all Products

**FEATURED SOLUTIONS**

Application Security

Building Management Systems

Cloud Security Posture Management

Compliance

Exposure Management

Finance

Healthcare

IT/OT

Ransomware

State / Local / Education

US Federal

Vulnerability Management

Zero Trust

Community & Support

Customer Education

Tenable Research

Documentation

Trust and Assurance

Nessus Resource Center

Cyber Exposure Fundamentals

System Status

**CONNECTIONS**

Blog

Contact Us

Careers

Investors

Events

Media

Privacy Policy Legal 508 Compliance