#! Anatomy of a Bug

Autopsy of CVSS 9.3

EternalBlue

The Patient

- **Name:** Windows SMBv1 Driver (srv.sys)
- **CVE:** CVE-2017-0144
- **Diagnosis:** Integer Overflow & Type Confusion
- **Vector:** Remote
- **Severity:** 🔥 9.3

What does 9.3 mean?

- **Auth:** None.
- **User Interaction:** None.
- **Attack Vector:** Remote.
- **Result:** Immediate Ring 0 (SYSTEM) execution.

#1 The Context

Origin of a Cyber Weapon

#1.1 The Context

Origin of a Cyber Weapon

👉 Developer: The Equation Group (attributed to the NSA).

👉 Leak: April 2017, by The Shadow Brokers.

👉 Significance:

- 👉 Not a commodity vulnerability.
- 👉 Military-grade exploit.
- 👉 Protocol-layer weaponization, bypassing perimeter defenses.

#1.2 The Context

Global Kinetic Impact

👉 WannaCry (May 2017).

👉 Wormable ransomware via EternalBlue.

👉 UK NHS, Spanish telecoms, global logistics crippled.

👉 NotPetya (June 2017).

👉 Nation-state wiper disguised as ransomware.

👉 ≈ $10 billion in damages (Maersk, Merck, FedEx).

👉 Lesson: Once a state exploit leaks, it becomes a global systemic risk immediately.

#2 The Architecture

The SMB Protocol

#2.1 The Architecture

SMBv1 in Kernel Space

👉 SMB: Core Windows Networking fabric.

👉 SMBv1: Legacy protocol from the 1980s (CIFS).

👉 Supports OS/2 File Extended Attributes (FEA).

👉 Risk: To support obsolete OS/2 clients, modern Windows retained complex FEA parsing logic inside the kernel.

#2.2 The Architecture

Kernel Pool Allocation

👉 **NonPagedPool:** Kernel memory that cannot be paged out.

👉 srv.sys: SMB request handler.

👉 Incoming packets allocate directly from NonPagedPool.

👉 Impact: Corrupt the pool → corrupt the kernel.

#3 The Vulnerability

Three Bugs, One Exploit

#3.1 The Vulnerability

Bug A — Integer Truncation

👉 Function: SrvOs2FeaListSizeToNt

👉 Purpose: Calculate required buffer size for FEA conversion.

👉 Calculation uses DWORD (32-bit).

👉 Return value cast to WORD (16-bit).

👉 Failure:

- 👉 65537 → 1
- 👉 Allocates 1 byte
- 👉 Copies 65,537 bytes

👉 Classic kernel integer overflow.

#3.2 The Vulnerability

Bug B — Transaction Type Confusion

👉 Goal: Send >64KB payloads.

👉 Start with SMB_COM_NT_TRANSACT (32-bit size).

👉 Continue with SMB_COM_TRANSACTION2_SECONDARY (16-bit logic).

👉 Validation uses initial 32-bit type.

👉 Processing uses secondary 16-bit constraints.

👉 Result: Data is copied under incompatible assumptions.

#3.3 The Vulnerability

Bug C — Heap Grooming Primitive

👉 **Vector:**
SMB_COM_SESSION_SETUP_ANDX

👉 **Mode: Extended Security, zero negotiation.**

👉 **ByteCount parsed from wrong offset.**

👉 **Triggers oversized NonPagedPool allocation.**

👉 **Result: alloc → free → predictable kernel hole.**

#4 The Kill-Chain

Kernel Heap Feng Shui

#4.1 The Kill-Chain

Phase 1 — The Spray

👉 **Action:**

- 👉 **15+ concurrent TCP connections.**
- 👉 **Streams 1–13 send SMB_COM_TRANSACTION2.**

👉 **Purpose:**

- 👉 **Fill existing fragmentation.**
- 👉 **Force contiguous future allocations.**

#4.2 The Kill-Chain

Phase 2 — The Hole

👉 Stream 14:

👉 Trigger Bug C.

👉 Allocate ≈ 0x11000 bytes.

👉 Close connection.

👉 Result:

👉 Kernel frees the chunk.

👉 Precise hole surrounded by controlled data.

#4.3 The Kill-Chain

Phase 3 — The Overwrite

👉 Stream 0:

- 👉 Send malicious FEA list.
- 👉 Sized to fit exactly into the hole.

👉 Payload:

- 👉 Header: 0x10000
- 👉 Item 606: large data block
- 👉 Item 607: bridge object (0xA8)

👉 Trigger:

- 👉 Bug A fires.
- 👉 Copy overruns into adjacent object header.

#4.4 The Kill-Chain

Phase 4 — Execution (DoublePulsar)

👉 Target: SRVNET_BUFFER

👉 Overwrite:

- 👉 Corrupt function pointer.
- 👉 Redirect to shellcode.

👉 Implant:

- 👉 Kernel-mode backdoor
- 👉 Hooks KernelCallbackTable
- 👉 DLL injection into lsass.exe.

👉 Result: Silent, persistent Ring 0 RCE.

#5 The Fix.

Kernel Patching

#5.1 The Fix.

The Vulnerable Logic

```
DWORD calculatedSize = SrvOs2FeaListSizeToNt(feaList);

// Truncation bug
WORD allocatedSize = (WORD)calculatedSize;

buffer = ExAllocatePoolWithTag(
    NonPagedPool,
    allocatedSize,
    'LSBF'
);

// Overflow
MoveMemory(buffer, feaList, calculatedSize);
```

#5.2 The Fix.

The Patched Logic

```
DWORD calculatedSize = SrvOs2FeaListSizeToNt(feaList);

// This.
if (calculatedSize > 0xFFFF) {
    return STATUS_INVALID_PARAMETER;
}

WORD allocatedSize = (WORD)calculatedSize;
```

#6 Developer's Takeaway

Kernel Math is Law

#6.1 Developer’s Takeaway

Kernel Math is Law

👉 Never trust client-supplied size or length fields.

👉 Track bytes written, not allocated memory.

👉 Remove legacy / compatibility code from hot paths.

👉 Disable unused features (code = attack surface).

👉 Assume info leaks lead to full compromise.

Status

Patched (April 2017).
MS17-010.
SMBv1 disabled by default on Windows 11.

#! Anatomy of a Bug

Technical Credits:

Microsoft MSRC

Author: @tralsesec

#HeapGrooming #KernelExploit #NSA #Ring0 #SMBv1 #EternalBlue