

# [UNIX] University of Minnesota Gopher do\_command Buffer Overflow Vulnerability

*Source:* <http://www.derkeiler.com/Mailing-Lists/Securiteam/2003-07/0101.html>

---

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

*Date:* 07/24/03

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

Date: 24 Jul 2003 15:43:59 +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 in Canada

Toronto-based Sunrays Technologies is now Beyond Security's representative in Canada.

We welcome ISPs, system integrators and IT systems resellers

to promote the most advanced vulnerability assessment solutions today.

Contact us at 416-482-0038 or at [canadasales@beyondsecurity.com](mailto:canadasales@beyondsecurity.com)

-----

University of Minnesota Gopher do\_command Buffer Overflow Vulnerability

---

## SUMMARY

The [<ftp://boombox.micro.umn.edu/pub/gopher/>](ftp://boombox.micro.umn.edu/pub/gopher/) UMN gopher server. This server is "a robust and full-featured gopher and gopher+ server with a HTTP mode as well. It features support for indexing, ASK blocks, .Links files, .names files, .cap support, and pretty much any gopher feature you could imagine". A buffer overflow in the Gopherd's do\_command() function allows remote attackers to cause the program to execute arbitrary code.

## DETAILS

Vulnerable systems:

\* UMN Gopherd version 3.0.5 and prior

Vulnerable code:

In Gopherd.c /do\_command() you can see:

..

```
CMDfromNet(cmd, sockfd);
```

```
..
```

```
if (authpw == NULL || authuser == NULL)
    Die(sockfd, 411, "Missing Username or password");
    /* End else */
    } else {
    authuser = CMDgetAskline(cmd, 0);.....ponit
    authpw = CMDgetAskline(cmd, 1);
    }
```

```
..
```

```
case AUTHRES_OK:
```

```
    Gticket = (char*) malloc(sizeof(char*) *
        (strlen(authuser) +
        strlen(authpw)+5));
    strcpy(cleartext, authuser); .....ponit
    strcat(cleartext, " ");
    strcat(cleartext, authpw);
```

```
...
```

```
command.h/ #define CMDgetAskline(a,b) (STAGetText((a)->asklines,b))
```

```
...
```

Therefore there is an unchecked length of the strcpy() function.

#### ADDITIONAL INFORMATION

The information has been provided by <mailto:nic0x333@hotmail.com> nic.

```
=====
```

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.