

[UNIX] Cyrus IMSP Remote Root Vulnerability

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2003-12/0054.html>

From: SecuriTeam (support_at_securiteam.com)

Date: 12/18/03

To: list@securiteam.com

Date: 18 Dec 2003 12:46:31 +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>

Cyrus IMSP Remote Root Vulnerability

SUMMARY

Cyrus IMSP is a implementation of the [<http://asg.web.cmu.edu/cyrus/rfc/imsp.html>](http://asg.web.cmu.edu/cyrus/rfc/imsp.html) IMSP protocol. The Internet Message Support Protocol (IMSP) is "designed to support the provision of mail in a medium to large scale operation. It is intended to be used as a companion to the IMAP4 protocol [IMAP4], providing services which are either outside the scope of mail access or which pertain to environments which must run more than one IMAP4 server in the same mail domain. The services that IMSP provides are extended mailbox management, configuration options, and address books".

There is a remotely exploitable buffer overflow in the Cyrus IMSPd. The vulnerability can be triggered before authentication. The IMSP daemon is required to run as root.

DETAILS

Vulnerable systems:

* IMSP versions 1.4, 1.5a6, 1.6a3, and 1.7

Immune systems:

* IMSP versions 1.6a4, and 1.7a

Securiteam: [UNIX] Cyrus IMSP Remote Root Vulnerability

In the function `abook_dbname`, a `sprintf()` call takes place. The function takes two char pointers (`dbname` and `name`), which are later used in the `sprintf()` call:

```
sprintf(dbname, abookdb, ownerlen, name, name);
```

`abookdb` is defined as

```
static char abookdb[] = "user/%.*s/abook.%s";
```

Several functions in the code use `abook_dbname()` and supply a local char buffer of 256 bytes as first argument to the function. Since the second argument "name" is controlled by the user in several protocol messages, a remotely exploitable buffer overflow is created.

Solution:

Andrew Systems Group has released new versions. Older versions are no longer supported.

<<ftp://ftp.andrew.cmu.edu/pub/cyrus/cyrus-imsdp-v1.6a4.tar.gz>>

<ftp://ftp.andrew.cmu.edu/pub/cyrus/cyrus-imsdp-v1.6a4.tar.gz>

<<ftp://ftp.andrew.cmu.edu/pub/cyrus/cyrus-imsdp-v1.7a.tar.gz>>

<ftp://ftp.andrew.cmu.edu/pub/cyrus/cyrus-imsdp-v1.7a.tar.gz>

And

<<http://ftp.andrew.cmu.edu/pub/cyrus/cyrus-imsdp-v1.6a4.tar.gz>>

<http://ftp.andrew.cmu.edu/pub/cyrus/cyrus-imsdp-v1.6a4.tar.gz>

<<http://ftp.andrew.cmu.edu/pub/cyrus/cyrus-imsdp-v1.7a.tar.gz>>

<http://ftp.andrew.cmu.edu/pub/cyrus/cyrus-imsdp-v1.7a.tar.gz>

Vendor communication:

08.12.2003 Initial notification

08.12.2003 Rob Siemborski answers

08.12.2003 Rob Siemborski sends a patch

09.12.2003 n.runs tests the patch and finds it to be correct

09.12.2003 CERT VU# assigned

12.12.2003 Rob Siemborski sends the new versions

15.12.2003 public release

ADDITIONAL INFORMATION

The information has been provided by <<mailto:felix.lindner@nrns.com>>

Felix Lindner.

=====

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

=====

=====

Securiteam: [UNIX] Cyrus IMSP Remote Root Vulnerability

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.