

[UNIX] Rsync Heap Overflow

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2003-12/0019.html>

From: SecuriTeam (support_at_securiteam.com)

Date: 12/04/03

To: list@securiteam.com

Date: 4 Dec 2003 20:10:30 +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>

Rsync Heap Overflow

SUMMARY

The rsync team has received evidence that a vulnerability in rsync was recently used in combination with a Linux kernel vulnerability to compromise the security of a public rsync server. While the forensic evidence we have is incomplete, we have pieced together the most likely way that this attack was conducted and we are releasing this advisory as a result of our investigations to date.

Our conclusions are that:

- * rsync version 2.5.6 and earlier contains a heap overflow vulnerability that can be used to remotely run arbitrary code

- * While this heap overflow vulnerability could not be used by itself to obtain root access on a rsync server, it could be used in combination with the recently announced brk vulnerability in the Linux kernel to produce a full remote compromise

- * The server that was compromised was using a non-default rsyncd.conf option "use chroot = no". The use of this option made the attack on the compromised server considerably easier. A successful attack is almost certainly still possible without this option, but it would be much more difficult.

Securiteam: [UNIX] Rsync Heap Overflow

Please note that this vulnerability only affects the use of rsync as a "rsync server". To see if you are running an rsync server you should use the netstat command to see if you are listening on TCP port 873. If you are not listening on TCP port 873 then you are not running a rsync server.

DETAILS

Vulnerable systems:

- * rsync version 2.5.6 and prior

Immune systems:

- * rsync version 2.5.7

New rsync release:

In response we have released a new version of rsync, version 2.5.7. This is based on the current stable 2.5.6 release with only the changes necessary to prevent this heap overflow vulnerability. There are no new features in this release.

We recommend that anyone running an rsync server take the following steps:

1. Update to rsync version 2.5.7 immediately.
2. If you are running a Linux kernel prior to version 2.4.23 then you should upgrade your kernel immediately. Note that some distribution vendors may have patched versions of the 2.4.x series kernel that fix the brk vulnerability in versions before 2.4.23. Check with your vendor security site to ensure that you are not vulnerable to the brk problem.
3. Review your /etc/rsyncd.conf configuration file. If you are using the option "use chroot = no" then remove that line or change it to "use chroot = yes". If you find that you need that option for your rsync service then you should disable your rsync service until you have discussed a workaround with the rsync maintainers on the rsync mailing list. The disabling of the chroot option should not be needed for any normal rsync server.

The patches and full source for rsync version 2.5.7 are available from <http://rsync.samba.org/> and mirror sites. We expect that vendors will produce updated packages for their distributions shortly.

Solution:

```
* <http://samba.org/ftp/rsync/rsync-2.5.7.tar.gz> rsync-2.5.7.tar.gz (
<http://samba.org/ftp/rsync/rsync-2.5.7.tar.gz.sig> signature),
<http://samba.org/ftp/rsync/rsync-2.5.6-2.5.7.diff.gz>
rsync-2.5.6-2.5.7.diff.gz (
<http://samba.org/ftp/rsync/rsync-2.5.6-2.5.7.diff.gz.sig> signature).
```

ADDITIONAL INFORMATION

The rsync team would like to thank the following individuals for their assistance in investigating this vulnerability and producing this response: <<mailto:tss.iki.fi>> Timo Sirainen, <<mailto:mhw.wittsend.com>>

Securiteam: [UNIX] Rsync Heap Overflow

Mike Warfield, <mailto:rusty.samba.org> Paul Russell, and
<mailto:lcars.gentoo.org> Andrea Barisani.

=====

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.