

o has made new Samba packages available, closing two buffer overflow security holes that may allow arbitrary code to be e

> [Linux Reviews](#) > [News and headlines](#) > [2004 News archive](#) > [July](#) >

SuSE and Gentoo has made new Samba packages available, closing two buffer overflow security holes that may allow arbitrary code to be executed.

2004-07-23, xiando

A buffer overflow vulnerability is present in the base64 code of The Samba Web Administration Tool (SWAT) in Samba version 3.0.2 to 3.0.4. It may allow remote attackers to execute arbitrary code before any authorization has taken place. Another buffer overflow in Samba 2.2.x, Samba 3.0.0 and later version is present if you are using mangling method = hash in smb.conf.

The default setting is mangling method = hash2 in smb.conf, and this method is not vulnerable.

The [Samba](#) Web Administration Tool (SWAT) allows you to easily manage and configure Samba through a web interface. It is called through xinetd and you may want to disable it (disable = yes in /etc/xinetd.d/swat) until you have upgraded if you are currently using Samba version 3.0.2 to 3.0.4. Try `http://localhost:901/` to find out if you are running SWAT on your computer.

A safe Samba-3.0.5 ebuild that fixes these buffer overruns was added to [Gentoo portage](#) 2004-07-22.
(`emerge sync && emerge net-fs/samba`)

Packages for [SuSE Linux](#) are now available.

From SuSE's announcement:

The Samba Web Administration Tool (SWAT) was found vulnerable to a buffer overflow in its base64 code. This buffer overflow can possibly be exploited remotely before any authentication took place to execute arbitrary code.

The same piece of vulnerable code was also used in `ldapsam passdb` and in the `ntlm_auth` tool.

This vulnerability only exists on Samba 3.0.2 to 3.0.4.

Another buffer overflow was found in Samba 3.0.0 and later, as well as in Samba 2.2.x. This overflow exists in the hash code of the mangling method (`smb.conf: mangling method = hash`), the default uses `hash2` which is not vulnerable.

There is no temporary workaround known. The first proof-of-concept exploits were seen on public mailing lists.

After the installation was successfully completed please restart the samba daemon.

```
/usr/sbin/rcsmb restart
```

SWAT is called by `inetd/xinetd`. Therefore it is sufficient to kill all running instances of SWAT only.

Please download the update package for your distribution and verify its integrity by the methods listed in section 3) of this announcement. Then, install the package using the command `"rpm -Fhv file.rpm"` to apply

SuSE and Gentoo has made new Samba packages available, closing two buffer overflow security holes tha

has made new Samba packages available, closing two buffer overflow security holes that may allow arbitrary code to be e

the update.

Our maintenance customers are being notified individually. The packages are being offered to install from the maintenance web.

Note that SLES8 packages will be delivered with a short delay.

- [SUSE-SA-2004-022](#)

> [Linux Reviews](#) > [News and headlines](#) > [2004 News archive](#) > [July](#) >

SuSE and Gentoo has made new Samba packages available, closing two buffer overflow security holes that may allow arbitrary code to be executed.

SuSE and Gentoo has made new Samba packages available, closing two buffer overflow security holes tha