Date: Mon, 26 Apr 2021 15:21:16 +0200
From: Matthias Gerstner <mgerstner@...e.de>
To: oss-security@...ts.openwall.com
Subject: virtualbox: CVE-2021-2264: vboxautostart-service.sh allows injection
 of parameters in 'su' invocation

Hello,

I recently discovered an issue in the script "vboxautostart-service.sh"
which is distributed by Oracle as part of their virtualbox RPMs [1]. By
default this script is not used but it can be enabled by an
Administrator according to the manual [2].

In the context of the autostart feature a directory "$VBOXAUTOSTART_DB"
(by default /etc/vbox) is used. Local users in the system are granted
write access to this directory. Users are supposed to create files of
the form "<username>.start" to configure autostarting of their
respective virtualbox VMs.

The version of the script in virtualbox release 6.1.18 (and older
releases) runs as root and uses the following bash for loop in its
`start()` function:

```
    for user in `ls $VBOXAUTOSTART_DB/*.start`
    do
        start_daemon `basename $user | sed -ne "s/\(.*\).start/\1/p"` $binary $PARAMS > /dev/null 2>&1
    done

    [...]

    start_daemon() {
        usr="$1"
        shift
        su - $usr -c "$*"
    }
```

Since by design unprivileged users need to have write access to this
directory, an unprivileged user can create arbitrarily named new files
in it that will be processed by the for loop above.

If a user creates a file like "$VBOXAUTOSTART_DB/--evil.start", then the
for loop will pass "--evil" as parameter to `start_daemon()`, resulting
in the command line flag `--evil` being passed to the `su` utility. A
reproducer for the openSUSE virtualbox package, which uses an older but
similarly vulnerable autostart script, looks like this:

```
    # emulate a malicious user that is a member of the vboxusers group
    root# su -g vboxusers nobody
    nobody$ cd /etc/vbox
    # try to inject a parameter to 'su'
    nobody$ touch -- '-s myshell.start'
    nobody$ exit
    # execute the autostart script
    root# /usr/lib/virtualbox/vboxautostart.sh start
    vboxautostart.sh: Starting VirtualBox VMs configured for autostart.
    vboxautostart.sh: Starting VMs for user -s myshell.
    # execution fails, because we cannot embed '/' characters in
    # filenames
    su: failed to execute  myshell: No such file or directory
```

Luckily this is not a full local root exploit. Two aspects are reponsible for
this:

- filenames cannot contain '/' characters, therefore we cannot specify
  any valid executable beyond the CWD (usually "/") of the autosart.sh script.
- the $user argument is passed before the `-c /usr/lib/virtualbox/VBoxAutostart`
  parameter. And the command line parsing logic of 'su' lets the final
  `-c` parameter win, i.e. the attacker cannot influence the command that is run.

Still a local attacker can specify arbitrary other parameters to `su` this way
e.g. the `--group=mygroup` parameter. It could be a successful attack vector
when combined with other security issues.

Beyond this any member of the vboxusers group can influence the autostart
settings of other users, as long as the victim user is allowed to
autostart via /etc/vbox/autostart.cfg.

On a more generic level this design of /etc/vbox as "autostart DB"
allows any member of the vboxusers group to trigger a run of
/usr/lib/virtualbox/VBoxAutostart as any local user (by influencing the
$user value) or as root with any local group (by setting $user to
--group=mygroup).

I privately reported this issue to Oracle Security on 2021-04-08. It has
been fixed via a critical patch update by upstream on 2021-04-20. The
fixed version of the script has stronger limitations on the accepatble
*.start filenames and also requires that the username present in the
file matches the owner of the file.

The openSUSE packages for virtualbox are about to receive updates [3].

[1]: https://www.virtualbox.org/wiki/Linux_Downloads
[2]: https://www.virtualbox.org/manual/ch09.html#autostart-linux
[3]: https://bugzilla.suse.com/show_bug.cgi?id=1184542

Cheers

Matthias

--
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)**