Date: Wed, 14 Sep 2022 11:56:48 +0200
From: Matthias Gerstner <mgerstner@...e.de>
To: oss-security@...ts.openwall.com
Subject: insufficiently protected D-Bus interface in KDiskMark 3.0.0
 (CVE-2022-40673)

Introduction

The SUSE security team has been asked to review changes [1] in the D-Bus
implementation in KDiskMark [2] major version 3.0.0. KDiskMark is a graphical
utility that allows to run performance benchmarks on local file systems.

Vulnerability

The review of this codebase showed that the D-Bus interface of the privileged
helper program `kdiskmark_helper` is insufficiently secured. Only the helper's
`init()` member function (helper.cpp:51) is protected by the Kauth
framework and thus by Polkit `auth_admin` authentication. Calling the `init()`
method, once authorized, causes the actual Helper D-Bus interface to be
registered on the D-Bus system bus. This means that the usual D-Bus level
autostart of the helper service is not possible, but only users in the system
that authenticate as root are allowed to fully start the helper.

Once the helper *is* started, however, all further D-Bus methods offered by
the helper interface are *not* protected any more. Any user with access to the
D-Bus system bus may invoke them without restrictions. These D-Bus methods
then offer attack surface:

- removeFile: allows to remove arbitrary files in the system (local DoS,
              arbitrary file existence test).
- prepareFile: allows to create large files owned by root in arbitrary locations
               (also via symlinks), the final path component needs to be
               .kdiskmark.tmp, if not, then kdiskmark itself is DoS'ed, because
               it quits.
- startTest: similar to prepareFile. No arbitrary code execution is possible,
             because the interface takes mostly integers as input and the
             `fio` sub process command line is carefully constructed.
- flushPageCache: drops the kernel's file system caches, therefore this offers
             a kind of local performance DoS.

Fixed Version

I informed the review requestor (who is also the upstream author) about the
issue and upstream created a follow-up version 3.1.0 featuring a
fixed approach to authentication.

I obtained CVE-2022-40673 from Mitre to track the lack of proper D-Bus method
authentication in the D-Bus helper program.

Timeline

2022-08-24: review request for KDiskMark 3.0.0 reached us.
2022-08-31: I started working on the review.
2022-08-31: I informed the upstream author about the vulnerability, offering
            coordinated disclosure and a suggestion on which approach to take
            to fix it.
2022-09-07: Upstream presented version 3.1.0 with an improved
            authentication scheme.
2022-09-12: I performed a follow-up review and found the vulnerability to be
            fixed.
2022-09-13: I requested a CVE for the issue from Mitre.
2022-09-14: There was no formal embargo established, upstream published fixes
            for the issue right away. Publication of the CVE, Bugzilla bug and
            full report on our end.

```
# References

[1]: https://bugzilla.suse.com/show_bug.cgi?id=1202725
[2]: https://github.com/JonMagon/KDiskMark.git

Cheers

Matthias

--
Matthias Gerstner <matthias.gerstner@...e.de>
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: Ivo Totev, Andrew Myers, Andrew McDonald, Boudien Moerman
```

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