Bug 1259401 (CVE-2026-25704) - AUDIT-TRACKER: CVE-2026-25704: cosmic-greeter: new D-Bus service configured in om.system76.CosmicGreeter.conf

Status: IN_PROGRESS

Alias: CVE-2026-25704

Product: openSUSE Tumbleweed
Component: Security (show other bugs)
Version: Slowroll
Hardware: Other Other

Priority: P5 - None **Severity**: Normal (vote)
Target Milestone: ---
Assignee: Matthias Gerstner
QA Contact: E-mail List

URL:
Whiteboard:
Keywords:

Depends on:
Blocks:

- Clone This Bug

Reported: 2026-03-09 14:11 UTC by Richard Rahl
Modified: 2026-04-08 11:38 UTC (History)
CC List: 2 users (show)

See Also:
Found By: ---
Services Priority:
Business Priority:
Blocker: ---

Attachments

Add an attachment (proposed patch, testcase, etc.)

Note

You need to log in before you can comment on or make changes to this bug.

Richard Rahl 2026-03-09 14:11:02 UTC Description

```
Hi security team,
I would like to request a dbus service file audit for cosmic-greeter
(https://build.opensuse.org/package/show/X11:COSMIC:Factory/cosmic-greeter,
upstream is https://github.com/pop-os/cosmic-greeter), as this is the last step
before I can push it to Factory.

Thanks in advance
```

Matthias Gerstner 2026-03-09 14:45:07 UTC Comment 1

```
Thank you for creating the bug. We will look into it.
```

The rpmlint diagnostic is as follows:

```
> cosmic-greeter.x86_64: E: dbus-file-unauthorized (Badness: 10)
>     /usr/share/dbus-1/system.d/com.system76.CosmicGreeter.conf (sha256 file diges
>    [...]
>    xml filter:1ebea85b767776514a33e00cd238ba620b507a2077fea6b4c2c677466b9f3332)
```

The configuration only allows members of the "cosmic-greeter" group to talk to the D-Bus service. The service is implemented in Rust and consists of about 5,000 lines of code.

Matthias Gerstner 2026-03-10 13:00:35 UTC Comment 2

The D-Bus service, as I mentioned before, is only accessible for members of the "greeter" group. There only D-Bus method available on the interface is

    com.system76.CosmicGreeter.GetUserData

This method has some issues, though. It collects all user accounts in the system and then processes the user-owned Cosmic configuration files in their home directories. The authors of the code were aware of the risks in this approach, which they tried to solve by dropping privileges to the owner of the home directory which is about to be processed.

The privilege drop is incomplete, however: the daemon runs with full root privileges and has no systemd hardening applied. The privilege drop only changes the effective user ID of the process, but keeps the group ID of 0. This means an attacker can still attempt to perform exploits based on the root group privileges of the daemon.

The D-Bus service attempts to lookup configuration files, create directories and process configuration files in various locations of unprivileged users' home directories. It uses racy checks to determine the file type, which provide a time window for symlink attacks and Denial-of-Service attacks.

The severity of the issues is reduced, because a potential attacker has to wait for somebody to invoke the problematic D-Bus method. Still these issues should be addressed before we accept the daemon in openSUSE.

Please keep this information private until further notice. I will reach out to upstream and discuss the further security disclosure process with them.

Here is an excerpt from the strace calls involving the problematic file system accesses in my test case:

```
[pid  3348] setresuid(-1, 1000, -1 <unfinished ...>
[pid  3348] <... setresuid resumed>)    = 0
[pid  3348] statx(AT_FDCWD, "/var/lib/AccountsService/icons/mgerstner",
AT_STATX_SYNC_AS_STAT, STATX_ALL, 0x7feb5d5f8a50) = -1 ENOENT (No such file or
directory)
[pid  3348] statx(AT_FDCWD,
"/home/mgerstner/.local/share/cosmic/com.system76.CosmicTheme.Mode/v1",
AT_STATX_SYNC_AS_STAT, STATX_ALL, 0x7feb5d5f8800) = -1 ENOENT (No such file or
directory)
[pid  3348]
mkdir("/home/mgerstner/.config/cosmic/com.system76.CosmicTheme.Mode/v1", 0777) = -1
EEXIST (File exists)
[pid  3348] statx(AT_FDCWD,
"/home/mgerstner/.config/cosmic/com.system76.CosmicTheme.Mode/v1",
AT_STATX_SYNC_AS_STAT, STATX_ALL, {stx_mask=STATX_ALL|STATX_MNT_ID,
stx_attributes=0, stx_mode=S_IFDIR|0755, stx_size=4096, ...}) = 0
[pid  3348] statx(AT_FDCWD,
"/home/mgerstner/.config/cosmic/com.system76.CosmicTheme.Mode/v1/is_dark",
AT_STATX_SYNC_AS_STAT, STATX_ALL, {stx_mask=STATX_ALL|STATX_MNT_ID,
stx_attributes=0, stx_mode=S_IFCHR|0666, stx_size=0, ...}) = 0
[pid  3348]
mkdir("/home/mgerstner/.config/cosmic/com.system76.CosmicTheme.Dark/v1", 0777) = -1
EEXIST (File exists)
[pid  3348] openat(AT_FDCWD,
```

```
"/home/mgerstner/.config/cosmic/com.system76.CosmicTheme.Dark/v1/palette",
O_RDONLY|O_CLOEXEC) = 11
[pid  3349] setresuid(-1, 0, -1 <unfinished ...>
```

Matthias Gerstner 2026-03-11 12:25:35 UTC Comment 3

```
I established contact to an upstream developer and system76 security. I
forwarded a formal report to them. I will provide more information as soon as
I know more details about the process.
```

Matthias Gerstner 2026-03-11 13:56:00 UTC Comment 4

```
Upstream does not want to follow coordinated disclosure, thus we can go fully
public now. Let's see when there's an improved version available from upstream. We
might also assign a CVE for the issue.
```

Johannes Segitz 2026-03-11 16:05:11 UTC Comment 6

```
Use CVE-2026-25704 for the
CWE-271: Privilege Dropping / Lowering Errors
issue
```

Matthias Gerstner 2026-03-12 09:36:00 UTC Comment 7

```
Here is my take on CVSS scores and CWE categories:

CWE-271: Privilege Dropping / Lowering Errors
CWE-367: Time-of-check Time-of-use (TOCTOU) Race Condition

CVSS:3.1/AV:L/AC:H/PR:L/UI:N/S:U/C:L/I:L/A:H (score=5.8)
CVSS:4.0/AV:L/AC:H/AT:N/PR:L/UI:N/VC:L/VI:L/VA:H/SC:N/SI:N/SA:N (score=5.8)
```

Matthias Gerstner 2026-03-13 09:54:08 UTC Comment 8

```
Upstream communicated to us that there is no more need to keep this private, they
published information already on their GitHub.
```

Matthias Gerstner 2026-03-13 10:31:29 UTC Comment 9

```
Upstream is working on a bugfix here:

https://github.com/pop-os/cosmic-greeter/pull/426

I provided them some feedback already by email.
```

Matthias Gerstner 2026-03-24 10:10:03 UTC Comment 11

```
The first part of the bugfix has been merged into the upstream repository.
This makes things already quite a bit better. There is still some protection
against local DoS missing, which I already discussed with upstream 10 days
ago. I'm not seeing any activity currently to address this, thus I just pinged
upstream again for the current status.
```

Matthias Gerstner 2026-04-08 11:38:39 UTC Comment 12

There has just been created a 1.0.9 version tag in the upstream repository. I still don't see a bugfix for the remaining Denial-of-Service attack surface. When you package the 1.0.9 version we can still consider whitelisting the service in its current form. The local Denial-of-Service is less severe and also cannot be actively triggered by unprivileged users (as far as I know).

Format For Printing - XML - Clone This Bug - Top of page