



[skip to content](#)  
[Back to GitHub.com](#)

 [Security Lab](#)  
[Bounties](#) [Research](#) [Advisories](#) [Get Involved](#) [Events](#)  
  
[Home](#) [Bounties](#) [Research](#) [Advisories](#) [Get Involved](#) [Events](#)  
November 9, 2020

# GHSL-2020-202: Local Privilege Escalation (LPE) in Ubuntu gdm3 - CVE-2020-16125



[Kevin Backhouse](#)

## Summary

gdm3 can be tricked into launching `gnome-initial-setup`, enabling an unprivileged user to create a new user account for themselves. The new account is a member of the `sudo` group, so this enables the unprivileged user to obtain admin privileges.

The vulnerability in gdm3 is triggered when the accountsservice daemon is unresponsive. I have simultaneously reported a separate denial-of-service vulnerability in accountsservice to Ubuntu. On Ubuntu 20.04.1 LTS, I am able to use the vulnerability in accountsservice to trigger the vulnerability in gdm3 and escalate privileges. As far as I know, the vulnerability in accountsservice only exists on Ubuntu. The freedesktop and debian versions of accountsservice do not contain the vulnerable code. However, gdm3 may also be vulnerable on other systems if a different way can be found to block D-Bus communication with the accountsservice daemon.

## Product

gdm3

## Tested Version

- gdm3, version 3.36.3-0ubuntu0.20.04.1
- Tested on Ubuntu 20.04.1 LTS
- Tested with accountsservice, version 0.6.55-0ubuntu12~20.04.1

## Details

### Issue 1: gdm3 LPE due to unresponsive accounts-daemon (GHSL-2020-202, CVE-2020-16125)

[gnome-initial-setup](#) is an application that is run on freshly installed systems. It presents a series of dialog boxes to the user, enabling them to create a new account on the machine. The newly created account is an admin account (it is a member of the `sudo` group). `gnome-initial-setup` is invoked by gdm3 when there are no user accounts on the machine. Therefore, if we can trick gdm3 into thinking that there are no user accounts, then it will launch `gnome-initial-setup`, enabling us to gain root privileges.

gdm3 uses a D-Bus method call to get the list of existing users from the accountsservice daemon, in [look for existing users sync](#):

```
static void
look_for_existing_users_sync (GdmDisplay *self)
{
    GdmDisplayPrivate *priv;
    GError *error = NULL;
    GVariant *call_result;
    GVariant *user_list;

    priv = gdm_display_get_instance_private (self);
    priv->accountsservice_proxy = g_dbus_proxy_new_sync (priv->connection,
                                                         0, NULL,
                                                         "org.freedesktop.Accounts",
                                                         "/org/freedesktop/Accounts",
                                                         "org.freedesktop.Accounts",
                                                         NULL,
                                                         &error);

    if (!priv->accountsservice_proxy) {
        g_warning ("Failed to contact accountsservice: %s", error->message);
        goto out;
    }

    call_result = g_dbus_proxy_call_sync (priv->accountsservice_proxy,
                                          "ListCachedUsers",
                                          NULL,
                                          0,
                                          -1,
                                          NULL,
                                          &error);

    if (!call_result) {
        g_warning ("Failed to list cached users: %s", error->message);
        goto out;
    }

    g_variant_get (call_result, "(@ao)", &user_list);
    priv->have_existing_user_accounts = g_variant_n_children (user_list) > 0;
    g_variant_unref (user_list);
    g_variant_unref (call_result);

out:
    g_clear_error (&error);
}
```

It seems that the value of `priv->have_existing_user_accounts` is false by default, so if the D-Bus method call fails (due to a timeout) then it will remain false. You will see the message “Failed to list cached users” in the system log.

`look_for_existing_users_sync` is called from [gdm display prepare](#):

```
gboolean
gdm_display_prepare (GdmDisplay *self)
{
    GdmDisplayPrivate *priv;
    gboolean ret;

    g_return_val_if_fail (GDM_IS_DISPLAY (self), FALSE);

    priv = gdm_display_get_instance_private (self);

    g_debug ("GdmDisplay: Preparing display: %s", priv->id);

    /* FIXME: we should probably do this in a more global place,
     * asynchronously
     */
    look_for_existing_users_sync (self);

    priv->doing_initial_setup = wants_initial_setup (self);

    g_object_ref (self);
    ret = GDM_DISPLAY_GET_CLASS (self)->prepare (self);
    g_object_unref (self);

    return ret;
}
```

If `priv->have_existing_user_accounts` is false, then `wants_initial_setup` returns true, leading to the invocation of `gnome-initial-setup`.

## Impact

This issue may lead to local privilege escalation, where an unprivileged user is able to gain root privileges.

## Remediation

I recommend making the default value of `priv->have_existing_user_accounts` `true`.

## CVE

- CVE-2020-16125

## Coordinated Disclosure Timeline

- 2020-10-17: Reported to GNOME gdm: <https://gitlab.gnome.org/GNOME/gdm/-/issues/642>
- 2020-10-18: Also reported to gdm3 package on Ubuntu: <https://bugs.launchpad.net/ubuntu/+source/gdm3/+bug/1900314>
- 2020-10-19: Acknowledged by Marc Deslauriers (Ubuntu). No response yet from GNOME.
- 2020-10-20: CVE-2020-16125 assigned by Seth Arnold (Ubuntu).
- 2020-10-26: Marc Deslauriers (Ubuntu) asked if I had heard from GNOME yet.
- 2020-10-26: I email [security@gnome.org](mailto:security@gnome.org) to ask about the status of [issue 642](#).
- 2020-10-26: Replies received from Tobias Mueller and Ray Strobe at GNOME.
- 2020-10-27: Fix implemented by Marco Trevisan (GNOME): [https://gitlab.gnome.org/GNOME/gdm/-/merge\\_requests/117](https://gitlab.gnome.org/GNOME/gdm/-/merge_requests/117)
- 2020-10-27: Disclosure date agreed with GNOME and Ubuntu: 2020-11-03
- 2020-11-03: Issue disclosed by Ubuntu: <https://ubuntu.com/security/notices/USN-4614-1>
- 2020-11-03: GNOME bug report made publicly visible: <https://gitlab.gnome.org/GNOME/gdm/-/issues/642>
- 2020-11-06: Exploit explained by Alex Murray on the [Ubuntu Security Podcast](#).

## Credit

This issue was discovered and reported by GHSL team member [@kevinbackhouse \(Kevin Backhouse\)](#).

## Contact

You can contact the GHSL team at [securitylab@github.com](mailto:securitylab@github.com), please include a reference to GHSL-2020-202 in any communication regarding this issue.

## GitHub

## Product

- [Features](#)
- [Security](#)
- [Enterprise](#)
- [Customer stories](#)
- [Pricing](#)
- [Resources](#)

## Platform

- [Developer API](#)
- [Partners](#)
- [Atom](#)
- [Electron](#)
- [GitHub Desktop](#)

## Support

- [Docs](#)
- [Community Forum](#)
- [Professional Services](#)
- [Status](#)
- [Contact GitHub](#)

## Company

- [About](#)
- [Blog](#)
- [Careers](#)
- [Press](#)
- [Shop](#)

- 
- 
- 
- 
- 

- © 2021 GitHub, Inc.
- [Terms](#)
- [Privacy](#)
- [Cookie settings](#)