Closed Issue created 2 years ago by **Kevin Backhouse**

gdm3 privilege escalation due to unresponsive accounts-daemon (GHSL-2020-202)

GitHub Security Lab (GHSL) Vulnerability Report: `GHSL-2020-202`

The GitHub Security Lab team has identified a potential security vulnerability in gdm3.

We are committed to working with you to help resolve this issue. In this report you will find everything you need to effectively coordinate a resolution of this issue with the GHSL team.

If at any point you have concerns or questions about this process, please do not hesitate to reach out to us at `securitylab@github.com` (please include `GHSL-2020-202` as a reference).

If you are *NOT* the correct point of contact for this report, please let us know!

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`)

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.

I have made a video demonstrating the exploit, which you can see here. The video is only visible to people who have the link. Please note that the video also includes details of the vulnerability in accountsservice, so please be careful who you share it with.

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.

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`, please include a reference to `GHSL-2020-202` in any communication regarding this issue.

Disclosure Policy

This report is subject to our coordinated disclosure policy.

Drag your designs here or click to upload.

Tasks 0

No tasks are currently assigned. Use tasks to break down this issue into smaller parts.

Linked items 0

Related merge requests 1

display: Don't try to start gnome-initial setup on users check failure
!117

When this merge request is accepted, this issue will be closed automatically.

Activity

Kevin Backhouse @kevinbackhouse · 2 years ago Author

I have also reported this issue to Ubuntu: https://bugs.launchpad.net/ubuntu/+source/gdm3/+bug/1900314

They have assigned CVE-2020-16125 for this issue.

Edited by Kevin Backhouse 2 years ago

Ray Strode @halfline · 2 years ago Maintainer

Of course, if accountsservice is knocked out of commission, it's not going to be able to create users either.

So, exploiting this would require:

1. being able to gain local access to the system,
2. temporarily disable accountsservice through some sort of denial-of-service maneuver
3. then re-store accountsservice

I don't think it's unreasonable for GDM to rely on accountsservice being secured and functioning. If it's compromised, all bets are off, of course, which I believe mitigates this. Defaulting to assuming there are existing users seems okay to me as a security hardening measure.
@iainl @3v1n0 are you guys looking for any sort of embargo for this?

Marco Trevisan @3v1n0 · 2 years ago Developer

Mh, I do agree that assuming we've users is indeed the quickest and safest solution

Marco Trevisan @3v1n0 · 2 years ago Developer

As per the embargo thingy, I need to poke security I assume, we can prepare a fix meanwhile.

Michael Catanzaro @mcatanzaro · 2 years ago Developer

> So, exploiting this would require:
>
> 1. being able to gain local access to the system,
> 2. temporarily disable accountsservice through some sort of denial-of-service maneuver
> 3. then re-store accountsservice

Looks like Kevin's blog post shows how to do precisely that.

Michael Catanzaro @mcatanzaro · 2 years ago Developer

Er, actually step 3 is unclear. I'm not sure how does accountsservice start working again?

Kevin Backhouse @kevinbackhouse · 2 years ago Author

accounts-daemon is started on-demand by dbus-daemon. dbus-daemon is connected to accounts-daemon by a unix socket, which is how dbus-daemon keeps track of whether there is already an accounts-daemon running. When the first accounts-daemon crashes, the socket disconnects so dbus-daemon knows that accounts-daemon is no longer running. The next time that somebody tries to send a D-Bus message to accounts-daemon, it triggers dbus-daemon to start up a new accounts-daemon process.

Please register or sign in to reply

Marco Trevisan mentioned in merge request !117 (merged) 2 years ago

Marco Trevisan @3v1n0 · 2 years ago Developer

Fix is ready, the issue will stay hidden till CRD (2020-11-03)

Edited by Marco Trevisan 2 years ago

Ray Strode @halfline · 2 years ago Maintainer

cc @marc.deslauriers

Ray Strode made the issue visible to everyone 2 years ago

Ray Strode closed via commit 3747d588 2 years ago

Marco Trevisan closed via commit dc823512 2 years ago

Marco Trevisan mentioned in commit 91b6babb 2 years ago

Marco Trevisan mentioned in commit e08852be 2 years ago

Marco Trevisan mentioned in commit dc823512 1 year ago

Ray Strode mentioned in commit 3747d588 1 year ago

Please register or sign in to reply