June 17, 2020

GHSL-2020-057: dbus file descriptor leak (DoS) - CVE-2020-12049

Kevin Backhouse

Summary

D-Bus has a file descriptor leak, which can lead to denial of service when the dbus-daemon runs out of file descriptors. An unprivileged local attacker can use this to attack the system dbus-daemon, leading to denial of service for all users of the machine.

Product

D-Bus (dbus-daemon)

Tested Version

1.12.2-1ubuntu1.1 (tested on Ubuntu 18.04.4 LTS)

Details: File descriptor leak in `_dbus_read_socket_with_unix_fds`

The function `_dbus_read_socket_with_unix_fds` contains the following code at dbus-sysdeps-unix.c, line 438:

```
if (m.msg_flags & MSG_CTRUNC)
  {
    /* Hmm, apparently the control data was truncated. The bad
       thing is that we might have completely lost a couple of fds
       without chance to recover them. Hence let's treat this as a
       serious error. */

    errno = ENOSPC;
    _dbus_string_set_length (buffer, start);
    return -1;
  }
```

The intention of this code is to handle the case where too many file descriptors are sent over the unix socket, causing the control data to get truncated. That could be a deliberate attempt by an attacker to cause a denial of service. The problem with the code is that some file descriptors may still have been received, even though the message has been truncated. So we need to make sure that those file descriptors are closed. Otherwise an attacker can cause us to quickly run out of file descriptors.

Impact

This issue can lead to a local denial of service attack: an unprivileged local attacker can make the system unusable for all users. For example, on Ubuntu 18.04.4 LTS, my proof-of-concept exploit prevents all users from logging in, because the login screen needs to send a D-Bus message, but the dbus-daemon is no longer able to send or receive any messages because it cannot create any new file descriptors.

CVE

- CVE-2020-12049

Coordinated Disclosure Timeline

This report was subject to the GHSL coordinated disclosure policy.

- 04/09/2020: reported to maintainer
- 06/04/2020: embargo lifted, issue public and fixed

Resources

- https://gitlab.freedesktop.org/dbus/dbus/-/issues/294#note_522136
- https://github.com/github/securitylab/tree/c8db365b3258df1c6fd12ff0f818115f46423e25/SecurityExploits/freedesktop/DBus-CVE-2020-12049

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 the GHSL-ID: `GHSL-2020-057` in any communication regarding this issue.

- Community Forum
- Professional Services
- Status
- Contact GitHub

Company

- About
- Blog
- Careers
- Press
- Shop

- 
-
- 
-
-