

CVE-2022-42010: dbus-daemon crashes when receiving message with incorrectly nested parentheses and curly brackets


[@everx](#) discovered that dbus-daemon and other uses of DbusServer can be crashed by sending a message containing a type-signature in which parentheses () , struct/tuple and curly brackets ({ } , dict-entry) are incorrectly nested.

This was originally reported in [a comment on #413](#), but it is not really related to [#413 \(closed\)](#), except that they are both denial-of-service vulnerabilities.

Here is a hex-dump of a reproducer that [@everx](#) provided:

```
$ xxd -ps minimized-from-e1f55a417825f05084b88a0aae8525e0fbb07075
6c8f2801000000007b22000818000000fd152874617b79617b64617b7961
7b7961717d7d297d0000000000000000000000c0000000000000000000
00000000feff0000
```

which contains invalid signature (ta{ya{da{ya{yaq}}}}). A more minimal reproducer would be (a{xy}).

 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](#) added [1.Crash](#) [1.Security](#) [libdbus](#) labels [1 month ago](#)

 [Simon McVittie](#) assigned to [@smcv](#) [1 month ago](#)

 [Simon McVittie](#) mentioned in issue [#413 \(closed\)](#) [1 month ago](#)


 [Simon McVittie](#) [@smcv](#) · [1 month ago](#) Author Owner

I have requested a CVE ID from MITRE.

 [Simon McVittie](#) [@smcv](#) · [1 month ago](#) Author Owner


CVE-2022-42010











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

 [Simon McVittie](#) changed title from **dbus-daemon crashes when receiving message with incorrectly nested parentheses and curly brackets** to **CVE-2022-42010: dbus-daemon crashes when receiving message with incorrectly nested parentheses and curly brackets** [1 month ago](#)

 [Simon McVittie](#) mentioned in commit [35d12acb](#) [1 month ago](#)

 [Simon McVittie](#) mentioned in commit [8f382ee4](#) [1 month ago](#)

 [Simon McVittie](#) mentioned in commit [992c0da4](#) [1 month ago](#)

-  **Simon McVittie** mentioned in commit [b9f914fa](#) 1 month ago
-  **Simon McVittie** mentioned in commit [fd73d1ef](#) 1 month ago
-  **Simon McVittie** mentioned in commit [6b88e768](#) 1 month ago
-  **Simon McVittie** mentioned in commit [c0bfcc09](#) 1 month ago
-  **Simon McVittie** mentioned in commit [67800ac5](#) 1 month ago
-  **Simon McVittie** mentioned in commit [d633016f](#) 1 month ago
-  **Simon McVittie** closed via commit [9d07424e](#) 1 month ago
-  **Simon McVittie** mentioned in commit [3e53a785](#) 1 month ago
-  **Simon McVittie** mentioned in commit [3ef34241](#) 1 month ago
-  **Simon McVittie** made the issue visible to everyone 1 month ago

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