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

<u>@evverx</u> 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

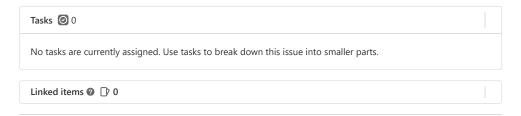
This was originally reported in <u>a comment on #413</u>, but it is not really related to <u>#413 (closed)</u>, except that they are both denial-of-service vulnerabilities.

Here is a hex-dump of a reproducer that <u>@evverx</u> provided:

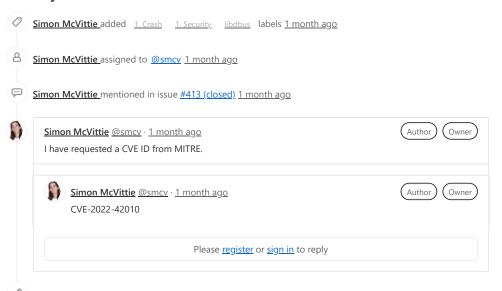
<pre>\$ xxd -ps minimized-from-e1f55a417825f05084b88a0aae8525e0fbb07075 6c8f2801000000007b22000818000000fd152874617b79617b64617b7961</pre>		
7b7961717d7d7d297d000000000000000000000000000000		
00000000feff0000		

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

⚠ Drag your designs here or <u>click to upload</u>.



Activity



<u>Simon McVittie</u> 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** <u>1 month ago</u>

- 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

(5)	Simon McVittie mentioned in commit b9f914fa 1 month ago
(F)	Simon McVittie mentioned in commit fd73d1ef 1 month ago
(F)	Simon McVittie mentioned in commit 6b88e768 1 month ago
(F)	Simon McVittie mentioned in commit cobfcco 1 month ago
	Simon McVittie mentioned in commit 67800ac5 1 month ago
(F)	Simon McVittie mentioned in commit d633016f 1 month ago
Θ	Simon McVittie closed via commit 9d07424e 1 month ago
(F)	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 <u>register</u> or <u>sign in</u> to reply