Fix issues found by static analysis #740

Merged ZoltanFridrich merged 1 commit into `p11-glue:master` from `ZoltanFridrich:zfridric_devel` on Jan 27

ZoltanFridrich commented on Jan 26 — Contributor

A slight overhaul of `p11_rpc_buffer_get_ibm_kyber_mech_param_update` and `p11_rpc_buffer_get_ibm_btc_derive_mech_param_update` functions where variable `data` could potentially be used uninitialized.

Report from static analysis:

```
1. Defect type: UNINIT
1. p11-kit-0.26.1/p11-kit/rpc-message.c:1706:2: var_decl: Declaring variable "data"
without initializer.
11. p11-kit-0.26.1/p11-kit/rpc-message.c:1732:5: uninit_use_in_call: Using uninitialized
value "data" when calling "memcpy". [Note: The source code implementation of the function
has been overridden by a builtin model.]
#  1730|
#  1731|            if (params->pCipher && params->ulCipherLen == len) {
#  1732|->              memcpy(params->pCipher, data, len);
#  1733|                 params->ulCipherLen = len;
#  1734|            } else {
```

```
2. Defect type: UNINIT
1. p11-kit-0.26.1/p11-kit/rpc-message.c:1706:2: var_decl: Declaring variable "data"
without initializer.
11. p11-kit-0.26.1/p11-kit/rpc-message.c:1735:5: uninit_use: Using uninitialized value
"data".
#  1733|                 params->ulCipherLen = len;
#  1734|            } else {
#  1735|->              params->pCipher = (void *) data;
#  1736|                 params->ulCipherLen = len;
#  1737|            }
```

```
3. Defect type: UNINIT
1. p11-kit-0.26.1/p11-kit/rpc-message.c:1776:2: var_decl: Declaring variable "data"
without initializer.
9. p11-kit-0.26.1/p11-kit/rpc-message.c:1797:4: uninit_use_in_call: Using uninitialized
value "data" when calling "memcpy". [Note: The source code implementation of the function
has been overridden by a builtin model.]
#  1795|
#  1796|        if (params->pChainCode && params->ulChainCodeLen == len) {
#  1797|->          memcpy(params->pChainCode, data, len);
#  1798|            params->ulChainCodeLen = len;
#  1799|        } else {
```

```
4. Defect type: UNINIT
1. p11-kit-0.26.1/p11-kit/rpc-message.c:1776:2: var_decl: Declaring variable "data"
without initializer.
9. p11-kit-0.26.1/p11-kit/rpc-message.c:1800:4: uninit_use: Using uninitialized value
"data".
#  1798|            params->ulChainCodeLen = len;
#  1799|        } else {
#  1800|->          params->pChainCode = (void *) data;
#  1801|            params->ulChainCodeLen = len;
#  1802|        }
```

ZoltanFridrich self-assigned this on Jan 26

ZoltanFridrich requested a review from **ueno** 3 months ago

ueno approved these changes on Jan 27

View reviewed changes

ueno left a comment — Member

LGTM

p11-kit/rpc-message.c — Show resolved

ifranzki approved these changes on Jan 27

View reviewed changes

ifranzki left a comment — Contributor

lgtm

`Fix issues found by static analysis` ··· ✗ `1ef4e45`

ZoltanFridrich force-pushed the `zfridric_devel` branch from **`bd95394`** to **`1ef4e45`** 3 months ago — Compare

ZoltanFridrich merged commit **`39f3b5e`** into `p11-glue:master` on Jan 27 — View details

13 of 14 checks passed

ZoltanFridrich added the bug label on Feb 6

sighook added a commit to zeppe-lin/pkgsrc-system that referenced this pull request on Feb 7

`[notify] p11-kit: 0.26.1 -> 0.26.2 (security)` ··· ✓ `1f1dc73`

mweinelt mentioned this pull request 2 weeks ago

p11-kit: 0.26.1 -> 0.26.2 NixOS/nixpkgs#495103

Merged

Reviewers

ueno ✓

+1 more reviewer

ifranzki ✓

Assignees

ZoltanFridrich

Labels

bug

Projects

None yet

Milestone

No milestone

Development

Successfully merging this pull request may close these issues.

None yet

3 participants