Bug 2437308 (CVE-2026-2100) - CVE-2026-2100 p11-kit: NULL dereference via C_DeriveKey with specific NULL parameters

Keywords: Security

Status: NEW

Alias: CVE-2026-2100

Product: Security Response

Component: vulnerability

Version: unspecified

Hardware: All

OS: Linux

Priority: medium

Severity: medium

Target Milestone: ---

Assignee: Product Security DevOps Team

QA Contact:

Docs Contact:

URL:

Whiteboard:

Depends On: ~~2437309~~ ~~2437310~~

Blocks:

TreeView+ depends on / blocked

Reported: 2026-02-06 12:06 UTC by OSIDB Bzimport

Modified: 2026-04-23 17:54 UTC (History)

CC List: 5 users (show)

Fixed In Version:

Clone Of:

Environment:

Last Closed:

Embargoed:

Attachments (Terms of Use)

OSIDB Bzimport 2026-02-06 12:06:01 UTC Description

```
Summary: potential NULL dereference in p11-kit when calling
C_DeriveKey remotely with specific parameters.

Requirements to exploit: if an attacker calls C_DeriveKey on a
remote token with either mechanism IBM kyber or IBM btc
derive, with specific mechanism parameter values set to NULL.
The RPC-client might attempt to return an uninitialized value
potentially resulting in a NULL dereference or undefined
behavior.


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|                }
```

Note

You need to log in before you can comment on or make changes to this bug.