author	Dan Carpenter <dan.carpenter@linaro.org>	2025-04-02 14:01:41 +0300
committer	Greg Kroah-Hartman <gregkh@linuxfoundation.org>	2025-04-25 10:47:41 +0200
commit	aaf356f872a60db1e96fb762a62c4607fd22741f (patch)	
tree	8246b03c19e267853ef7eca07db0bd77b23f322b	
parent	6ad0acb56b83492f01c6ba3f37c1335980eaa3f6 (diff)	
download	linux-aaf356f872a60db1e96fb762a62c4607fd22741f.tar.gz	

diff options

context: 3

space: include

mode: unified

Bluetooth: btrtl: Prevent potential NULL dereference

```
[ Upstream commit 324dddea321078a6eeb535c2bff5257be74c9799 ]

The btrtl_initialize() function checks that rtl_load_file() either
had an error or it loaded a zero length file.  However, if it loaded
a zero length file then the error code is not set correctly.  It
results in an error pointer vs NULL bug, followed by a NULL pointer
dereference.  This was detected by Smatch:

drivers/bluetooth/btrtl.c:592 btrtl_initialize() warn: passing zero to 'ERR_PTR'

Fixes: 26503ad25de8 ("Bluetooth: btrtl: split the device initialization into smaller parts")
Signed-off-by: Dan Carpenter <dan.carpenter@linaro.org>
Reviewed-by: Hans de Goede <hdegoede@redhat.com>
Signed-off-by: Luiz Augusto von Dentz <luiz.von.dentz@intel.com>
Signed-off-by: Sasha Levin <sashal@kernel.org>
```

Diffstat

-rw-r--r-- drivers/bluetooth/btrtl.c 2

1 files changed, 2 insertions, 0 deletions

```
diff --git a/drivers/bluetooth/btrtl.c b/drivers/bluetooth/btrtl.c
index 0a6ca6dfb94841..59eb9486642232 100644
--- a/drivers/bluetooth/btrtl.c
+++ b/drivers/bluetooth/btrtl.c
@@ -1215,6 +1215,8 @@ next:
                        rtl_dev_err(hdev, "mandatory config file %s not found",
                                    btrtl_dev->ic_info->cfg_name);
                        ret = btrtl_dev->cfg_len;
+                       if (!ret)
+                               ret = -EINVAL;
                        goto err_free;
                }
        }
```