Add sysno check in MessageReader

Browse files

```
The sysno in MessageReader is interpreted from the Message header passed
from the host. A malicious Message header may provide a modified sysno
to bypass the validation, and overwrites enclave memory. This change
adds a check for sysno to make sure it matches the expected value.

This issue was reported by Qinkun Bao, Zhaofeng Chen, Mingshen Sun, and
Kang Li from Baidu Security.

PiperOrigin-RevId: 377328054
Change-Id: I3ff6f60694d3390f66da89d139cf7cc7b49abaea
```

master
v0.6.3 buildenv-v0.6.3

kongoshuu committed on Jun 3, 2021 1 parent b0413b7 commit 90d7619e9dd99bcdb6cd28c7649d741d254d9a1a

Showing **1 changed file** with **3 additions** and **0 deletions**.

Split Unified

3 asylo/platform/system_call/system_call.cc

```
115 115     // Copy outputs back into pointer parameters.
116 116     auto response_reader =
117 117         asylo::system_call::MessageReader({response_buffer, response_size});
    118 +   if (response_reader.sysno() != sysno) {
    119 +     error_handler("system_call.cc: Unexpected sysno in response");
    120 +   }
118 121     const asylo::primitives::PrimitiveStatus response_status =
119 122         response_reader.Validate();
120 123     if (!response_status.ok()) {
```

0 comments on commit `90d7619`

Please sign in to comment.