

erlang / otp Public

<> Code Issues 368 Pull requests 142 Actions Projects Wiki

Commit 4e3bf86

u3s committed on Aug 27, 2025 Verified

ssh: verify file handle size limit for client data
- reject handles exceeding 256 bytes (as specified for SFTP)

master (#10156) · OTP-29.0-rc3 ··· OTP-27.3.4.3

1 parent c388a2d commit 4e3bf86

1 file changed +11

↑ Top

Filter files...

- lib/ssh/src
 - ssh_sftpd.erl

Search within code

lib/ssh/src/ssh_sftpd.erl

```

@@ -259,6 +259,17 @@ handle_data(Type, ChannelId, Data0, State =
#state{pending = Pending}) ->
259 259         handle_data(Type, ChannelId, Data, State#state{pending = <<>>})
260 260         end.
261 261
262 + %% From draft-ietf-secsh-filexfer-02 "The file handle strings MUST NOT be
    longer than 256 bytes."
263 + handle_op(Request, ReqId, <<?UINT32(HLen), _/binary>>, State = #state{xf = XF})
264 +     when (Request == ?SSH_FXP_CLOSE orelse
265 +           Request == ?SSH_FXP_FSETSTAT orelse
266 +           Request == ?SSH_FXP_FSTAT orelse

```

```
267 + Request == ?SSH_FXP_READ orelse
268 + Request == ?SSH_FXP_READDIR orelse
269 + Request == ?SSH_FXP_WRITE),
270 + HLen > 256 ->
271 + ssh_xfer:xf_send_status(XF, ReqId, ?SSH_FX_INVALID_HANDLE, "Invalid
    handle"),
272 + State;
262 273 handle_op(?SSH_FXP_INIT, Version, B, State) when is_binary(B) ->
263 274     XF = State#state.xf,
264 275     Vsn = lists:min([XF#ssh_xfer.vsn, Version]),
```



Comments 0



Please [sign in](#) to comment.