

Strict KEX Violations in Erlang/OTP SSH

Low

 u3s published GHSA-934x-xq38-hhqf 2 days ago

Package	Affected versions	Patched versions
No package listed	>=OTP 27.0 and	OTP 27.3.4
	<=OTP 27.3.3	OTP 26.2.5.12
	>=OTP 26.2.1	OTP 25.3.2.21
	and <=OTP	
	26.2.5.11	
	>=OTP 25.3.2.8	
	and <=OTP	
	25.3.2.20	
	>=OTP 24.3.4.15	
	>=OTP 23.3.4.20	
	>=OTP 22.3.4.27	

Severity

Low

 3.7 / 10

CVSS v3 base metrics

Attack vector	Network
Attack complexity	High
Privileges required	None
User interaction	None
Scope	Unchanged
Confidentiality	None
Integrity	Low
Availability	None

[Learn more about base metrics](#)

CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:L/A:N



CVE ID

CVE-2025-46712

Weaknesses

CWE-440

Credits

-  TrueSkrillor
- Finder
-  lambdafu
- Finder

Description

Summary

Erlang/OTP SSH fails to enforce strict kex handshake hardening measures by allowing optional messages to be exchanged. This allows a Man-in-the-Middle attacker to inject these messages in a connection during the handshake. As the optional messages are most likely to be ignored, there is no immediate security impact that we are aware of.

Details

draft-miller-sshm-strict-kex-01 states, that:

- When strict KEX is enabled, implementations MUST terminate the connection if they receive a non-KEX message during the initial key exchange. Permitted messages include only SSH_MSG_KEXINIT, SSH_MSG_NEWKEYS and the messages specific to each KEX algorithm:
- SSH_MSG_KEXDH_INIT and SSH_MSG_KEXDH_REPLY for the modp-DH diffie-hellman-* algorithms (Section 8 of [RFC4253]).

- SSH_MSG_KEX_DH_GEX_REQUEST_OLD, SSH_MSG_KEX_DH_GEX_REQUEST, SSH_MSG_KEX_DH_GEX_GROUP, SSH_MSG_KEX_DH_GEX_INIT and SSH_MSG_KEX_DH_GEX_REPLY for the Diffie Hellman group exchange
diffie-hellman-group-exchange-* algorithms (Section 5 of [RFC4419]).
- SSH_MSG_KEX_ECDH_INIT and SSH_MSG_KEX_ECDH_REPLY for ECDH KEX
algorithms defined in (Section 7.1 of [RFC5656]) and the hybrid Streamlined NTRUPrime/X25519 post-quantum KEM ([I-D.ietf-sshm-ntruprime-ssh]).
- SSH_MSG_KEX_HYBRID_INIT and SSH_MSG_KEX_HYBRID_REPLY for the
hybrid ML-KEM/ECDH algorithms ([I-D.ietf-sshm-mlkem-hybrid-kex]).

This condition is violated by Erlang/OTP SSH in the following ways (we ran our verification against the server implementation only, but message handling will likely be shared with the client implementation as well):

- After SSH_MSG_KEX_INIT, the client may send SSH_MSG_DEBUG, SSH_MSG_IGNORE, or SSH_MSG_UNIMPLEMENTED.
- After SSH_MSG_ECDH_INIT, the client may send SSH_MSG_DEBUG or SSH_MSG_UNIMPLEMENTED.
- SSH_MSG_KEX_DH_GEX_REQUEST does not correctly close the connection in non-DH GEX key exchanges. We are not sure how this message is handled, but from a protocol point of view the connection (presumably) switches over into an unrecoverable state, eventually leading to connection termination.

Impact

There is no immediate security risk to Erlang/OTP users that we are aware of. However, as this is a direct violation of draft-miller-sshm-strict-kex-01 as a security-relevant protocol extension, this may cause issues in the future.

Mitigation

- Users are advised to update to OTP-27.3.4 (for OTP-27), OTP-26.2.5.12 (for OTP-26), or OTP-25.3.2.21 (for OTP-25) to mitigate this issue.

Credits

Thanks to Fabian Bäumer, Marcel Maehren, Marcus Brinkmann, and Jörg Schwenk from the Ruhr University Bochum for finding and responsibly disclosing this vulnerability to the Erlang/OTP project.