Errata Slip #4
Proceedings of the 28th USENIX Security Symposium

For the paper "A Billion Open Interfaces for Eve and Mallory: MitM, DoS, and Tracking Attacks on iOS and macOS Through Apple Wireless Direct Link" by Milan Stute, *Technische Universität Darmstadt*; Sashank Narain, *Northeastern University*; Alex Mariotto, Alexander Heinrich, and David Kreitschmann, *Technische Universität Darmstadt*; Guevara Noubir, *Northeastern University*; Matthias Hollick, *Technische Universität Darmstadt* (Wednesday session, "Wireless Security," pp. 37–54 of the Proceedings) the authors would like to withdraw a statement in the discussion of the related work (Section 7.5) after correspondence with the authors of the cited paper [10]. The revised text is below.

Original:
Other attacks on AirDrop have been presented before. An impersonation attack [10] exploits mDNS/DNS-SD to redirect file transmissions to an attacker for unauthenticated connections. In particular, the attack uses forged SRV and AAAA responses to redirect an AirDrop ID to the attacker. In contrast to our work, [10] does not differentiate between authenticated and unauthenticated connections and claims that the UUID certificate (see Section 3.3) could not be bound to any contact identifiers, which we have found to be untrue. Also, the attack only works on unauthenticated connections, while our attack also targets authenticated connections via a downgrade attack and we present a complete MitM attack which allows an attacker to send malicious files to the receiver stealthily.

Revised:
Other attacks on AirDrop have been presented before. An impersonation attack [10] exploits mDNS/DNS-SD to redirect file transmissions to an attacker for unauthenticated connections. In particular, the attack uses forged SRV and AAAA responses to redirect an AirDrop ID to the attacker. This attack only affects unauthenticated connections, while our attack also targets authenticated connections via a downgrade attack and we present a complete MitM attack which allows an attacker to send malicious files to the receiver stealthily.

References:
[10] Xiaolong Bai, Luyi Xing, Nan Zhang, Xiaofeng Wang, Xiaojing Liao, Tongxin Li, and Shi-Min Hu. Staying Secure and Unprepared: Understanding and Mitigating the Security Risks of Apple ZeroConf. In *IEEE Symposium on Security and Privacy (S&P)*, May 2016. doi: 10.1109/SP.2016.45.