DirectTrust The most trusted name in health information exchange

Statement from DirectTrust regarding the EFAIL Vulnerability

Summary

EFAIL is a set of attacks used to exploit vulnerabilities in email clients that decrypt and display PGP and S/MIME encrypted messages by coercing them into sending the decrypted text of the emails to an attacker. Properly implemented, Direct is NOT vulnerable. However, we recommend that if you are exchanging with anyone outside of the DirectTrust Network, you will want to understand at a reasonable depth how their implementation protects against EFAIL.

How does EFAIL work?

EFAIL consists of two different attack scenarios that create "backchannels" to send the decrypted text to an attacker. Both require an attacker to first obtain the encrypted message.

1. The attacker "wraps" the encrypted body with carefully crafted markup that can result in an email client decrypting the message and sending the decrypted body to the attacker.
2. The attacker manipulates the encrypted body of the message using well known S/MIME weaknesses that produce a message that can send the decrypted body to the attacker once rendered in the email client.

Although the attacks are different, the end result is the same: a vulnerable email client sends the decrypted text to the attacker.

How is this relevant to Direct?

Direct uses S/MIME to encrypt messages, so in theory every Direct message could be vulnerable to this attack. However, Direct, when implemented correctly, is NOT vulnerable. The vulnerability is only applicable if decryption and rendering of the message are done in certain email clients like Thunderbird, iOS, Apple Mail, and some versions of Outlook. The best way to prevent EFAIL attacks is to decrypt S/MIME or PGP emails only in a separate application outside of your email client. For this purpose, a HISP is an external/separate application that decrypts messages and therefore removes the threat.

Why isn't Direct vulnerable?

While the S/MIME specification has multiple options to encrypt and digitally sign a message**,** the Direct specification mandates a very specific profile of S/MIME. It is this profile that protects Direct from the vulnerabilities of EFAIL.

1. The first attack scenario results in a message format that is non-compliant with the Direct specification. Proper implementations of Direct will immediately discard these messages.

1101 Pennsylvania Avenue NW
3rd Floor
Washington, DC 20004

DirectTrust.org
913.205.7968
www.directtrust.org

2. The second attack scenario results in manipulating the encrypted part of the message. Because Direct requires the use and validation of digital signatures, manipulating the encrypted message will result in an invalid message digest during the digital signature validation stage of the Direct protocol. Proper implementations of Direct will immediately discard these messages.

What has DirectTrust done to ensure proper implementations?

DirectTrust has implemented many safeguards to ensure proper implementations of Direct within its network:

- A detailed accreditation program that actively tests compliance of the Direct specification. This includes testing against the NIST test suite and DirectTrust testing tools that include several exception and vulnerability test cases.
- Ongoing yearly testing of every HISP in the network.
- A high bar of security and trust policies that must be met by both HISPs and Certificate Authorities.
- Due to security and trust risks in email clients, DirectTrust private key policies do not allow for both decryption and rendering of messages in email clients, which is a requirement for the EFAIL attacks to work. DirectTrust requires the HISP model.

What are the recommendations to protect against EFAIL?

1. You should utilize a HISP and not perform decryption inside of an email client.

2. If you are exchanging with anyone outside of the DirectTrust Network, you will want to understand at a reasonable depth how their implementation of Direct protects against EFAIL.

In summary, DirectTrust members can be assured that proper Direct implementations in combination with the security and trust policies of the DirectTrust Network are not vulnerable to EFAIL attack.