Efail: What A Disclosure FAIL That Was!

May 16, 2018 By RBS

Yesterday, news broke of a "critical" vulnerability in OpenPGP and S/MIME, named 'Efail' that could lead to an attacker gaining access to plaintext emails. News broke in the form of a dire warning from the Electronic Frontier Foundation warning people to "*immediately disable and/or uninstall tools that automatically decrypt PGP-encrypted email.*" This was, of course, picked up by various news outlets that ran with headlines varying from slightly alarming to factually wrong and embracing the hype. Potentially impacted vendors had to scramble fast, offering commentary on what the disclosure really means. Today, the researchers released the full paper, titled "*Efail: Breaking S/MIME and OpenPGP Email Encryption using Exfiltration Channels*".

In short, the researchers outline an attack scenario against OpenPGP and S/MIME that uses a combination of a known cryptographic attack along with mail clients that do not properly implement a MIME parser. The attack they outline requires access to the encrypted emails, which are then manipulated and sent to the victim. When the victim opens the email and decrypts the contents, a back-channel is established through the use of crafted content in an iframe that is not visible to the user. This general type of attack is well-known, but some email clients that implement OpenPGP or S/MIME may not throw the proper warnings when receiving modified cryptographic content. Overall, there is a high degree of complexity required to exploit these flaws, and it requires the victim to be running a vulnerable email client, load the crafted email, and decrypt the contents.

There are several components of this disclosure that are rooted in history. First, the cryptographic attacks against the Cipher Feedback Mode (CFB) (used by OpenPGP) and the Cipher Block Chaining (CBC) mode (used by S/MIME) have been known since 1999, and more generally known before that. Back in 2000, GnuPG implemented protection mechanisms to detect and warn about modified messages called Modification Detection Code (MDC), which will cause any message that has been modified to throw a clear error message warning th GnuPG has said that "ancient versions" (the 1.x line) may be susceptible to this, but any modern version (the 2.x line) is not. OpenPG implemented protection against malleability attacks since 2001 through the use of authenticated encryption (AE) called Modification

Detection Code (MDC). In the coming years, OpenPGP will be implementing a stronger form of AE (EAX or OCB depending on key preferences) that will better protect against these types of attacks. Finally, using iframes to hide content in email has long been used in a variety of spoofing attacks as well as companies using the method to track when an email is viewed.

When the actual paper was published, giving technical details of the vulnerability, it confirmed to many what GnuPG had already said and what was also echoed by an Enigmail developer. While there is an issue that may impact users in some situations, the notion that "*encrypted email isn't safe*" is certainly false!

This highlights an ongoing problem we see with vulnerability research that is done to garner as much media attention as possible before disclosing details. We wrote about this a couple years ago with the Badlock vulnerability, where like Efail, the hype and claims before disclosure didn't live up to the disclosure itself. When getting news coverage is more important than protecting organizations, such disclosures ultimately become a great disservice. Imagine organizations that caught wind of this vulnerability last night or this morning and began scrambling to figure out how to roll out mitigations based on the news articles. Is it really helpful if they disabled encrypted email across the entire organization? We don't think so. Forgoing all integrated email encryption on the slim chance you may be targeted with this attack just doesn't make sense.

In addition to the hype around the vulnerability, there are two more aspects of this disclosure we'd like to point out that further highlight the problem. First, the paper includes a list of 36 software-based email clients and 12 web-based clients offered via SaaS that are potentially susceptible. In that list, they say that Mailpile version 1.0.0rc2 is affected. However, according to the vendor, they explain why their software isn't vulnerable due to a list of defense-in-depth measures they had previously implemented (Note: one researcher disagrees with Mailpile, saying they are still vulnerable, and another disagrees with the disagreement). This calls into question the rest of their affected software list, especially on the back of finding out this vulnerability is not critical as claimed.

The second aspect of this disclosure that stands out to us is the last paragraph of their introduction, which states:

> **Responsible disclosure**. We have disclosed the vulnerabilities to all affected email vendors, and to national CERTs and our findings were confirmed by these bodies.

The notion that the researchers performed "responsible disclosure" with this vulnerability is frustrating and misleading. As Robert Hansen points out, he didn't receive a copy of the report from the researches, though another researcher disagrees saying Hansen was contacted in 2017. While they may have reached out to the impacted vendors, they apparently did not give them time to fix in some cases. Further, their contact with the GnuPG developers almost certainly included details that explained not only how they weren't vulnerable, but why the issue at hand was not as critical as they claimed. Yet, the paper was released after the news articles promoting how critical the issue supposedly was.

Additionally, we are long-time champions of the more accurate term of "coordinated disclosure" over "responsible disclosure". The idea of responsible disclosure was pushed heavily by Scott Culp at Microsoft back in October, 2001 and has become polarizing among many in Information Security. After years of pushing back, in 2010, Microsoft opted to drop the term as well due to the problems it caused.

There is a fine balance between using the press as an avenue for better awareness of a critical vulnerability. We understand the concept of naming a vulnerability and creating a web site for it as a one-stop clearinghouse for information on it. However, when time is spent doing that in a way that is misleading to organizations and may prompt them to make poor decisions that negatively impact their security posture, researchers must strongly evaluate their actions and improve their process going forward. This type of disclosure is a reminder that discussing disclosure issues, "responsible" or "coordinated", is relevant and timely.

Filed Under: News, Vulnerabilities Tagged With: Efail

Affordable SaaS security solution providing a complete Information Security Program with access to a CISO.

Risk Based Security's risk management solutions are a combination of data analytics, risk assessment and improvement strategies.

Not just security, the right security

Richmond, VA
(855) RBS-RISK
EMAIL US

Resources:

- VulnDB – Vulnerability Intelligence
- Cyber Risk Analytics
- YourCISO
- ISO/IEC 27001:2005 Pre-certification Consulting
- Security Intelligence Reports
- Risk Assessments
- Security Program Gap Analysis

About Us

Risk Based Security, incorporated in 2011, offers a full set of analytics and user-friendly dashboards designed specifically to identify security risks by industry.

Risk Based Security is the only company that offers its clients a fully integrated solution – real time information, analytical tools and purpose-based consulting.
[Read More...]

Latest News

- More Than 22,000 Vulnerabilities Disclosed In 2018
- Kick Off #RSAConference 2019 With Us
- RBS Is Heading To The RSA Conference, Are You?
- Over 6,500 Data Breaches and More Than 5 Billion Records Exposed in 2018
- VulnDB Add-On for Splunk Brings Best Vulnerability Intelligence To Risk Based Security and Splunk Customers
- Leaping Forward – Risk Based Security & JFrog Launch 2019 With A New Partnership
- Start the New Year Off Right! Join RBS in Exploring More from Cybersecurity to Cyber Risk at the 12th e-Crime & Cybersecurity Conference in Germany on January 23, 2019

Top of Page