Pentest®

PERFECT

Exploiting GMail SSL to Present the Original Certificate Chain in a Man-in-the-Middle Attack

Hugo Vázquez Caramés

www.pentest.es

2024

Exploiting GMail SSL to Present the Original Certificate Chain in a Man-in-the-Middle Attack

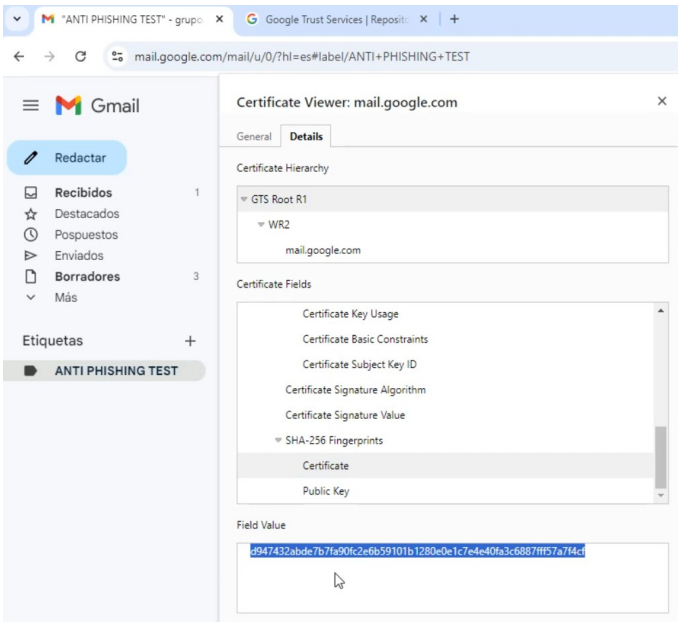
Hugo Vázquez Caramés, founder of PENTEST® - October 2024

https://www.pentest.es

1. INTRODUCTION: THE "PERFECT" VULNERABILITY

This paper introduces a critical security vulnerability dubbed "**Perfect**", referencing a "**Perfect Man-in-the-Middle" (MITM)**" attack. The vulnerability was discovered during a penetration test for a client and allows an attacker to:

1. **Execute a Man-in-the-Middle attack on SSL traffic.**
2. **Decrypt all SSL traffic** between the target and **GMail** (https://mail.google.com).
3. **Present the original certificate chain** in the browser, including the legitimate Root[2] and Intermediate CAs, making it impossible for users to detect the attack even through manual Inspection of the certificate chain.



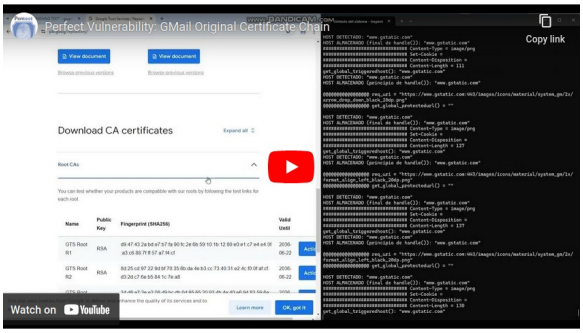
Despite contacting the vendor (Google), they have downplayed the vulnerability's significance, refusing to classify it as critical nor reward the disclosure.

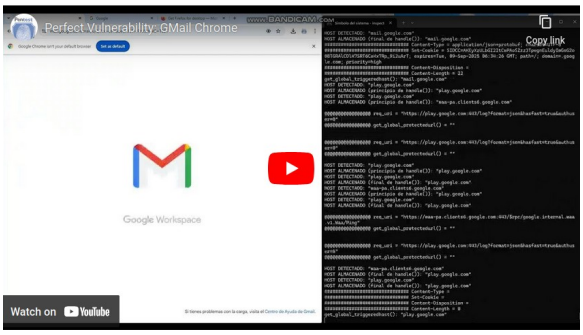
Given that over 1'5 billion users[3] are affected by the vulnerability, we are releasing our exploitation capability in this paper to raise awareness, without disclosing the exploit itself (which the vendor already possesses).

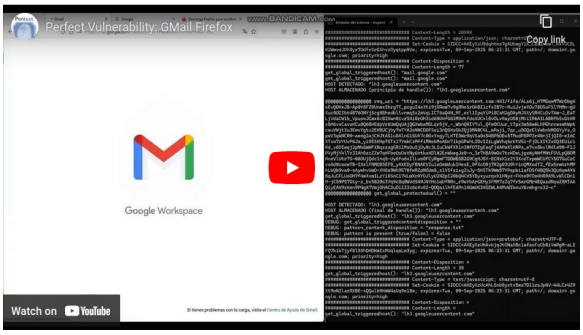
We provide several videos:

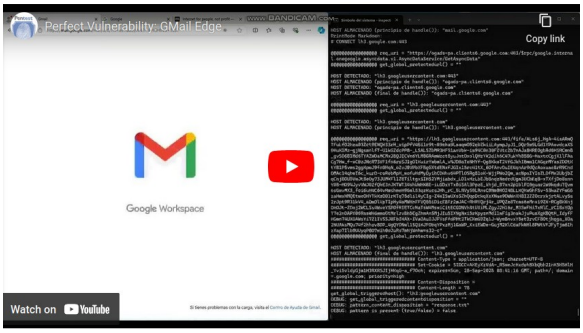
https://www.pentest.es/perfect_vulnerability.php

demonstrating the exploit in action and are open to discussions with companies or organizations with legitimate purposes, such as those involved in legal penetration testing, who wish to understand how to further weaponize this vulnerability.









2. THE "PERFECT" ATTACK: UNDERMINING SSL SECURITY

The "Perfect" vulnerability allows an attacker to perform an undetectable MITM attack by manipulating how SSL/TLS connections are handled by modern browsers and how they display SSL-related information to users.

2.1 Presentation of the Original Certificate Chain

In contrast to traditional MITM attacks, where rogue CAs raise browser warnings or cause certificate chain mismatches, this attack presents the original certificate chain, including the valid Root CA and Intermediate CA trusted by the target domain (https://mail.google.com). Even advanced users who inspect the certificate will be misled, as the chain appears perfectly legitimate.

In other MITM attacks, even if a rogue CA is installed and trusted by the browser, the user can manually detect the attack by checking the certificate chain against the vendor's declared PKI[4] information. The rogue CA would not match the legitimate Root and Intermediate CAs. However, the "**Perfect**" vulnerability makes this inspection useless, as the browser shows the authentic Root CA and Intermediate CAs, despite the connection being compromised.

This attack has been tested and confirmed across Chrome, Firefox, and Edge browsers. It is enabled by the specific way our exploit used for interception handles the target domain's SSL traffic and how the target domain implements its SSL configuration.

3. ATTACK VECTORS: TWO PRIMARY THREATS

The "Perfect" vulnerability can be exploited through two primary methods:

3.1 Rogue Root CA Implantation (Malware-based Attack)

Malware or an attacker can implant a rogue Root CA in the Windows user's profile certificate store, a process that does not require administrative privileges. Once this rogue CA is accepted, it can issue certificates for GMail (https://mail.google.com). The key risk here is that the original certificate chain is still displayed, deceiving users into thinking their connection is secure, while their traffic is intercepted and decrypted.

This scenario opens up the possibility of wide-scale exploitation by malware, intercepting SSL-encrypted data such as login credentials, personal information, or financial transactions—all while presenting the valid Root CA and Intermediate CA in the certificate chain.

3.2 Nation-State Attacks (Government-Controlled Root CAs)

In this specific case, nation-states that control a Root CA trusted by operating systems and browsers can issue SSL certificates for GMail (https://mail.google.com) and successfully execute the attack without having to implant any Root CA. This capability is not new, however, the critical point here is that for GMail (https://mail.google.com) they can execute the “Perfect” attack and achieve an undetectable Man-in-the-Middle. For other domains, even if a nation-state controls a trusted Root CA, the certificate chain will not be the original one, meaning that the browser will not display the legitimate Root and Intermediate CAs.

This limitation is key because it highlights that the "Perfect" vulnerability is tied to specific characteristics of the target domain’s (https://mail.google.com) client-server SSL implementation, making it much harder to replicate this type of attack on other domains, even with control over a trusted Root CA.

4. CRITICALITY OF THE VULNERABILITY

The "Perfect" vulnerability is especially critical because:

- **Undetectable to Users and Browsers**: While most MITM attacks can be detected by mismatched certificate chains or browser warnings, this attack retains the original certificate chain. As a result, neither the user nor the browser can detect the attack through standard inspection of the certificate.

- **Manual Inspection is Ineffective**: Even if a user manually inspects the SSL certificate, the Root CA and Intermediate CAs will match the vendor’s PKI. This bypasses one of the last lines of defense in SSL/TLS security—manual validation—since the presented certificate chain appears legitimate, even though the connection has been compromised.

- **Compromising GMail PKI Integrity**: Public Key Infrastructure (PKI) forms the backbone of SSL/TLS security, ensuring that users can trust the websites they connect to. The "Perfect" vulnerability undermines this trust by allowing an attacker to intercept GMail traffic while maintaining the original certificate chain, making the attack invisible to traditional detection methods.

5. IMPACT ON OVER 1'5 BILLION USERS

GMail is used by over 1'5 billion people globally. This vulnerability exposes all of these users to undetectable MITM attacks, without any indication of compromise.

The size of the user base, combined with the ease of exploiting this vulnerability, makes the impact far-reaching. The users of GMail, are at risk of having their secure communications compromised without their knowledge.

6. VENDOR'S RESPONSE

Despite being informed of the vulnerability, **Google has downplayed the issue (classified as "Won't fix")**, refusing to acknowledge its critical nature and rejecting to offer any kind of reward for its disclosure. This kind of response is concerning, as it leaves millions of users exposed to potential MITM attacks and despises current and future cyber security research work.

Given the vendor's inaction, it is crucial that this vulnerability be publicly disclosed so that users, security researchers, and organizations are aware of the risk and can take steps to mitigate it. The scope and severity of the vulnerability warrant urgent attention from the broader security community.

7. RATIONALE: WHY THIS GMAIL VULNERABILITY UNDERMINES PKI FUNDAMENTALS

The "Perfect" vulnerability fundamentally undermines the Public Key Infrastructure (PKI) that secures SSL/TLS communications. It breaks the very foundation of trust that PKI is built upon by allowing attackers to compromise connections while presenting the original certificate chain. Here's how:

- **Bypassing the Chain of Trust**: PKI ensures the authenticity of SSL certificates by linking them to trusted Root and Intermediate CAs. This vulnerability allows attackers to maintain the original chain of trust, deceiving both users and browsers into believing the connection is secure, even though the traffic is intercepted.

- **Rendering Certificate Validation Useless**: SSL/TLS certificate validation relies on checking the certificate chain against trusted Root and Intermediate CAs. In this case, the genuine Root and Intermediate CAs are shown to the user, so browsers validate the connection as secure, despite the fact that it has been compromised. This defeats the core purpose of SSL encryption, which is to protect users from MITM attacks.

- **Breaking the Integrity of SSL/TLS**: The vulnerability directly undermines the integrity of SSL/TLS encryption, as it allows attackers to intercept and decrypt communications while displaying the original certificate chain. This renders GMail SSL connections inherently untrustworthy, as users can no longer rely on SSL indicators or manual inspection to verify a secure connection.

8. CONCLUSION

The "Perfect" vulnerability exposes a significant flaw in SSL/TLS of GMail security and PKI trust models. By allowing attackers to intercept and decrypt SSL traffic while presenting the original certificate chain, this vulnerability makes it impossible for users or security tools to detect a MITM attack through conventional methods.

Given the massive user base of GMail and the fact that this vulnerability is undetectable by both browsers and users, the potential impact is enormous. The vendor’s refusal to address the issue only heightens the urgency for the security community to take action.

We encourage governments organizations involved in legal penetration testing or with legitimate purposes to reach out if they are interested in understanding how this vulnerability can be weaponized. Additionally, videos demonstrating the exploit has been made available to showcase its real-world impact.

This vulnerability highlights the fragility of SSL/TLS GMail (https://mail.google.com) security and the last mile of certificate validation. By presenting the genuine Root and Intermediate CAs while compromising the connection, this attack destroys the trust relationship that SSL/TLS GMail encryption was designed to protect.

9. AVAILABILITY FOR LEGITIMATE TESTING

We have prepared a dedicated demo environment where the "Perfect" vulnerability can be tested safely. Legitimate government organizations or any entity involved in legal Cybersecurity research are invited to contact us for more information. We can provide access to this environment to allow these organizations to verify the exploit's behavior and better understand its impact in a controlled setting. This allows qualified parties to see firsthand how the original certificate chain can be displayed during a man-in-the-middle attack and how this vulnerability could be easily weaponized.

REFERENCES

1. Certificate Authority. In Wikipedia, The Free Encyclopedia. Retrieved September 29, 2024, from https://en.wikipedia.org/wiki/Certificate_authority

2. Root Certificate. In Wikipedia, The Free Encyclopedia. Retrieved September 29, 2024, from https://en.wikipedia.org/wiki/Root_certificate

3. Gmail Statistics. Retrieved September 29, 2024, from https://techreport.com/statistics/software-web/gmail-statistics/

4. Public Key Infrastructure. In Wikipedia, The Free Encyclopedia. Retrieved September 29, 2024, from https://en.wikipedia.org/wiki/Public_key_infrastructure