GRADIENT

Securing Against the GoFetch Vulnerability in Apple Macs & Similar Encryption Key Leakages

WHITE PAPER

While Gradient's anchored credentials are completely secure against GoFetch-like attacks, ***any credentials used within the Gradient environment*** are short-lived and rendered infeasible targets for GoFetch-like attacks

Executive Summary

A recently discovered vulnerability, GoFetch, poses a significant threat to enterprise users of M-Series silicon MacBooks. This vulnerability allows attackers to potentially steal encryption keys, jeopardizing sensitive data. Gradient Cybersecurity Mesh (GCM) authentication anchors sensitive credentials to your device and makes them short-lived to secure you against this GoFetch vulnerability on Macs and other similar encryption key leakage attacks on any device.

Understanding GoFetch and its Implications

Potentially Severe Repercussions: The GoFetch vulnerability[1] is a recently discovered security flaw in Apple's M-series processor chips (M1, M2, M3) that allows attackers to potentially steal encryption keys from your Mac.[2] It works by exploiting a feature of the chip called the data memory-dependent prefetcher (DMP) which can leak information from the CPU cache under certain conditions. Most importantly, this vulnerability undermines the security measures typically used to protect encryption keys and, as the flaw is in the hardware, there doesn't appear to be an easy fix. Mitigations may be possible, but these might affect performance.

For enterprise IT professionals, the repercussions of a GoFetch exploit are severe. These keys are crucial for safeguarding data, and their compromise could result in unauthorized access to sensitive information. A successful attack could lead to data breaches, financial losses, and reputational damage.

How Attackers Can Exploit GoFetch to Steal Your Encryption Keys

In order to exploit the GoFetch vulnerability, the attacker first needs to place malicious software on the victim's device. This software, unlike some attacks, doesn't require administrator access (root access). A seemingly innocuous program with basic permissions can be enough. Phishing emails, applications designed to mimic legitimate software, or even compromised websites (watering hole attacks) could all be used to deliver this malicious software. Once installed, this software can exploit GoFetch to steal your highly sensitive, secret encryption keys without needing any further escalation of privileges.

To exploit the GoFetch vulnerability, the attacker only needs to place malicious software on the victim's device. Once installed, this software can exploit GoFetch to steal your highly sensitive, secret encryption keys without needing any further escalation of privileges.

[1] **GoFetch is summarized in an ArsTechnica article and detailed in the researchers' paper and website**

[2] **The security flaw was reportedly found in security flaw in Apple's M-series processor chips (M1, M2, M3); M-Series MacBooks were introduced in late 2020**

Gradient's Solution: Anchored and Short-Lived Credentials

Affordable and quick to implement in your environment, Gradient secures against the risks associated with GoFetch-like attacks through two key technologies:

Anchored Credentials eliminate the side channel exposure that GoFetch-like attacks leverage

For devices with supporting hardware, such as today's laptops and mobile phones, Gradient can leverage anchored credentials for authentication, for users, devices, endpoints, and sessions, securing these credentials so they can only be used from – and are anchored to – the user's device. These credentials store private keys within a Trusted Platform Module (TPM, as found on Windows devices) or Secure Enclave (as found on Apple products) on the device. These are hardware components specifically designed for secure key storage. All operations on the private key occur within this secure environment, rendering them inaccessible to malware or unauthorized processes running on the main processor. Since the keys never leave the TPM or Secure Enclave, GoFetch-like vulnerabilities cannot observe calculations made with them and therefore cannot exploit them.

Short-Lived, Anchored credentials limit the attack surface making GoFetch-like attacks infeasible

Gradient operates with short-lived credentials. These credentials, along with their associated keys, are only valid for minutes. The limited lifespan significantly reduces the window of opportunity for attackers to exploit them. The GoFetch research suggests that even a sophisticated attack would require significantly longer than the credential validity period to compromise commonly used keys (e.g., the researchers report that it takes 50 minutes for RSA 2048 and over two hours for Diffie-Hellman 2048). Furthermore, real-world attempts to exploit such vulnerabilities while remaining undetected would likely take even more time.

In essence, while anchored credentials are completely secure against GoFetch-like attacks, any credentials used within the Gradient environment are short-lived and rendered infeasible targets for GoFetch-like attacks.

Conclusion

The GoFetch vulnerability presents a serious challenge for enterprises relying on M-Series silicon MacBooks. Unfortunately, encryption key leakage attacks are not unique to these devices – and new ones will continually be discovered. Gradient's security solution effectively addresses this type of vulnerability by leveraging anchored and short-lived credentials. This comprehensive approach safeguards the encryption keys in Gradient credentials and mitigates the risks associated with GoFetch-like vulnerabilities.

APPENDIX: How GoFetch Works

GoFetch exploits a side-channel attack[1] specifically targeting processors with the data memory-dependent prefetchers (DMPs) found in Apple's M-Series silicon. These prefetchers try to anticipate data needs and pull them into the processor cache for faster access. Under specific conditions, the DMP in Apple's M-Series silicon will assume data in its memory cache is a pointer and proactively load the data pointed to by the "pointer" into the cache (note: while the processor doesn't really know if the data is a pointer or not, this DMP functionality will improve the performance of some types of software algorithms where address pointers are in memory). GoFetch works by crafting special inputs (for a target cipher algorithm) that manipulate the DMP. By analyzing how the DMP behaves (whether it activates or not), attackers can gradually infer bits of the secret key residing in the cache. Over many attempts, attackers can potentially reconstruct the entire key if specific bits are correctly guessed. However, this process is time-consuming, requiring repeated attempts and analysis. The cited research suggests an hour or more of continuous exploitation for common key lengths, making real-world attacks even more challenging, especially if needing to remain undetected (or, in Gradient's case, cracking the key before its short-term credentials expire).

[1] **A side-channel attack is a cyberattack that gleans information by analyzing indirect byproducts from a device, like electrical signals, timing variations, and memory residues, during its operations.**

What is Gradient

Gradient offers the only cybersecurity solution that continually protects and communicates, via patented secure hardware attestation, the complete security posture of every platform, all the way from the legitimacy of the hardware to the firmware (UEFI), kernel, kernel packages, and more, to establish a dynamic "fingerprint."

Gradient enhances the conventional authentication and conditional access flow for users, devices, and APIs to include the continual validation of both identity and the complete platform fingerprint. As a result, Gradient ensures that only legitimate users on valid, legitimate machines running correct, uncompromised software are allowed, where each of these attributes is re-evaluated at regular intervals to ensure they reflect the most up-to-date information on the state of every device on your network. This is dynamic attribute-based access control (ABAC) for everything, everywhere.