Apple Inc.

Vulnerability Report

Unauthorized Root Access in macOS Recovery Menu

Nicolas Steichen

Wednesday, May, 29th 2024

Table of Contents

Executive Summary......2
Recreation...... 3
Expected Behavior...... 6
Recommendation......7
Collaboration......9
Conclusion...... 10

Executive Summary

Vulnerability Summary:

A critical security vulnerability has been identified within the macOS Recovery menu firmware, allowing for unauthorized access to the root user terminal without requiring password authentication. This vulnerability poses a significant risk to the security and integrity of MacBook devices running macOS, as it enables malicious actors to gain unrestricted access to system resources and execute potentially harmful actions.

Notably, this vulnerability persists even when the device is in lockdown mode, underscoring the urgency of addressing the flaw to ensure comprehensive protection for MacBook users.

Discovery:

The discovery of this vulnerability stems from my extensive background as a computer enthusiast spanning over 12 years of relentless exploration and experimentation. My passion for tinkering with machines and bending them to my will, regardless of their intended limitations, has honed my skills, particularly in the realm of red teaming.

During an investigation aimed at removing all Apple firmware from a MacBook to install Linux, my curiosity led me deep into the system's firmware. It was during this exploration that I stumbled upon a critical flaw in the macOS Recovery menu. This flaw grants unrestricted access to the root user without the need for proper authentication, opening the door to potential exploitation by malicious actors.

Despite my relatively recent foray into formal studies of cybersecurity, the intricacies of computer systems feel instinctual to me. Understanding and uncovering vulnerabilities like this one comes naturally, driven by a deep-seated curiosity and a desire to push the boundaries of what's possible.

This discovery serves as a testament to the importance of continuous vigilance in identifying and addressing security vulnerabilities, ensuring the integrity and resilience of computer systems in the face of evolving threats.

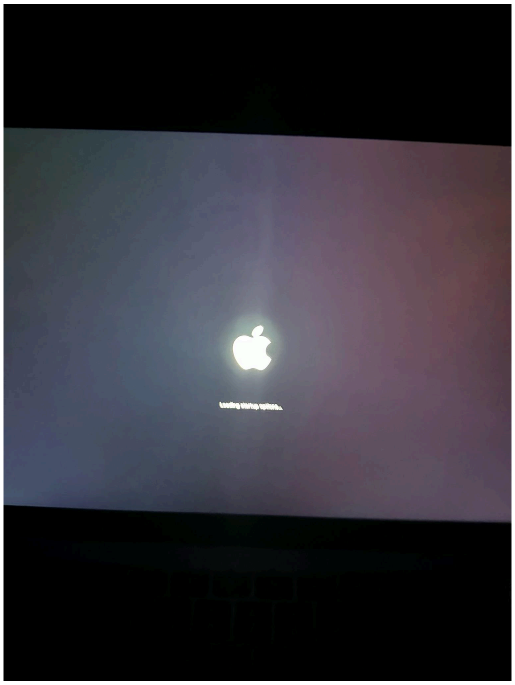
Recreation

Steps to Reproduce:

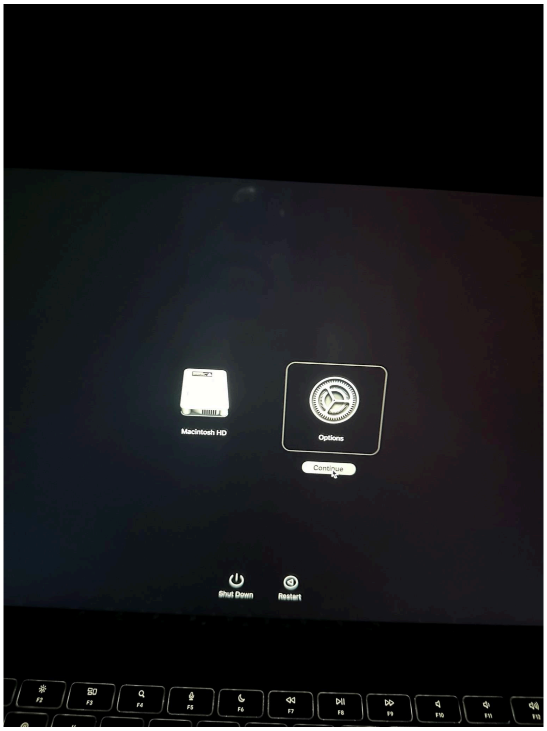
1. Shut down the MacBook to initiate the exploit.
2. Hold down the power button until the Apple logo appears, accompanied by the message "Loading startup options…".
3. In the startup options UI, click the "Options" gear icon and press continue.
4. You now have access to the macOS Recovery UI. By navigating to Utilities > Terminal or by using the shortcut 'Shift + Cmd + T' you have obtained unauthorized root access to the terminal.

Steps Visualized:

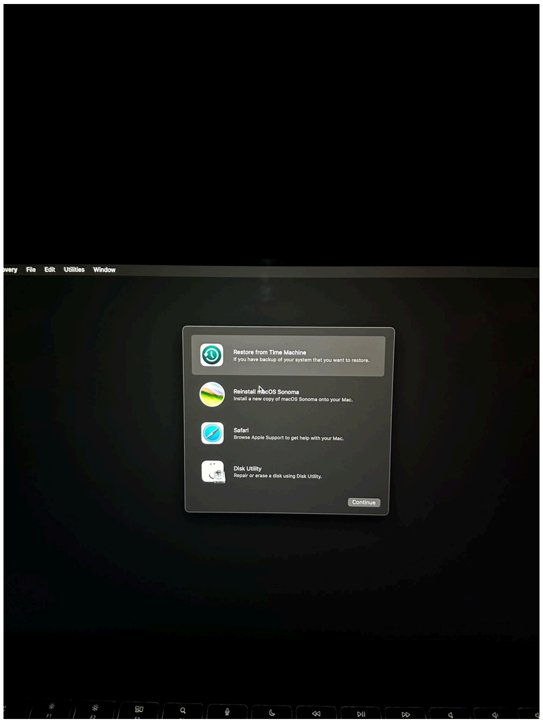
Step 1:



Step 2:



Step 3 (i have tested on multiple devices sometimes this happens sometimes it does not.):



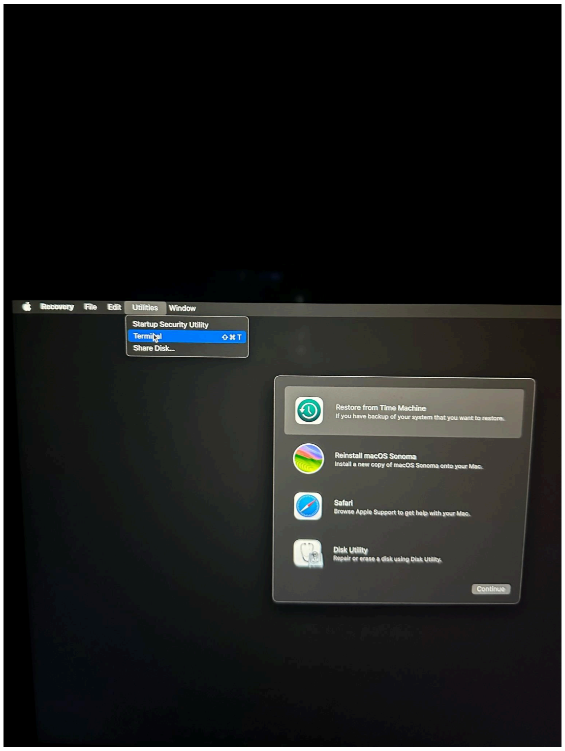
Restore from Time Machine
If you have backup of your system that you want to restore.

Reinstall macOS Sonoma
Install a new copy of macOS Sonoma onto your Mac.

Safari
Browse Apple Support to get help with your Mac.

Disk Utility
Repair or erase a disk using Disk Utility.

Step 4:



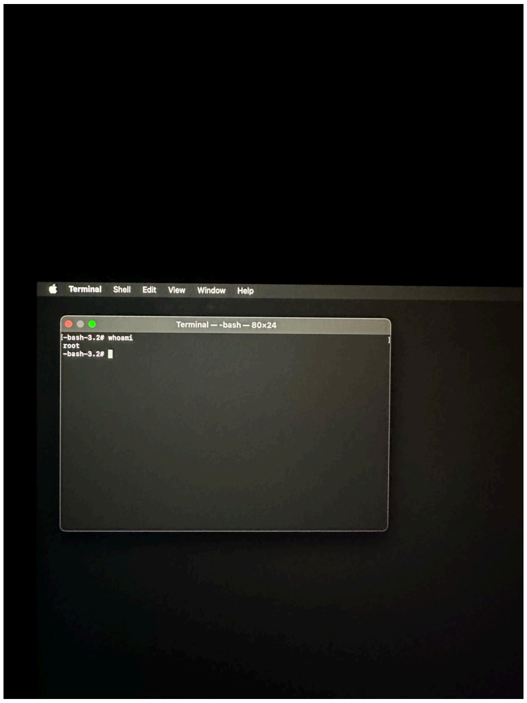
Restore from Time Machine
If you have backup of your system that you want to restore.

Reinstall macOS Sonoma
Install a new copy of macOS Sonoma onto your Mac.

Safari
Browse Apple Support to get help with your Mac.

Disk Utility
Repair or erase a disk using Disk Utility.

Step 5:



```
-bash-3.2# whoami
root
-bash-3.2# █
```

Expected Behavior

In a securely designed system, the access to any Terminal in macOS Recovery mode should mandatorily prompt for password authentication before granting root access. The absence of this crucial authentication step represents a significant security flaw.

For those unfamiliar with the ramifications of root level access on a machine, it grants the user unfettered control over the entire system. This level of access enables a malicious actor to execute a variety of devastating actions, including but not limited to:

Data Theft: Confidential information stored on the system, ranging from personal documents to sensitive corporate data, can be compromised, leading to privacy violations and potential identity theft.

System Manipulation: The ability to modify system configurations and tamper with critical files poses a serious risk of system instability, data loss, and potential rendering of the system inoperable.

Privilege Escalation: Exploiting this vulnerability can facilitate unauthorized access to other accounts or systems connected to the compromised macOS device, amplifying the scope of the security breach.

Network Exploitation: A malicious actor could leverage the compromised system to launch further attacks within the local network or on external networks, such as initiating Distributed Denial of Service (DDoS) attacks or spreading malware to other devices.

Persistent Backdoors: Unauthorized changes made to system configurations or the installation of backdoors could enable persistent access to the compromised system, allowing for continued unauthorized activity even after initial security measures are implemented.

Recommendation

Immediate action is imperative to address the identified vulnerability and fortify the security of MacBook users. To this end, I recommend that Apple's security team promptly initiate a comprehensive investigation to ascertain the root cause of the flaw and devise effective countermeasures to mitigate the associated risk.

As an additional layer of security, I propose the implementation of a password authentication requirement akin to the prompt for administrator credentials when executing privileged commands using 'sudo' or installing software that necessitates significant system alterations. This approach would bolster the security of macOS Recovery mode by ensuring that only authorized users with proper authentication can access the root privileges, thereby minimizing the potential for unauthorized exploitation of the system.

By swiftly addressing this vulnerability and implementing robust security measures, Apple can reaffirm its commitment to prioritizing user security and safeguarding the integrity of its products against emerging threats.

Collaboration

Responsible Disclosure:

The researcher intends to report this vulnerability to Apple's security team for further investigation and resolution. The vulnerability should be disclosed responsibly to ensure that appropriate remediation steps are taken without exposing users to potential security threats.

Collaboration Offer:

Furthermore, it is worth noting that while this vulnerability has been observed in MacBook devices, it is possible that it affects all macOS systems. As the researcher, I am committed to contributing to the enhancement of Apple's product security. I am willing to collaborate with Apple's security team to conduct further testing, identify vulnerabilities, and assist in the development of solutions to strengthen the security of macOS. By working together, we can ensure that macOS users are protected against potential threats and vulnerabilities.

Conclusion

The discovery of this vulnerability underscores the importance of robust security measures in all aspects of system firmware. While digital security measures are crucial, it's essential not to overlook the significance of physical security. Physical access to a device can often be the last resort for threat actors attempting to compromise a system. As such, implementing effective physical cyber security measures is imperative to complement digital safeguards. Prompt action is necessary to address this critical issue and prevent potential exploitation by malicious actors, reinforcing the need for a holistic approach to system security.