BLACKSWAN
CYBERSECURITY

THREAT ADVISORY

October 26, 2023

Multiple Vulnerabilities in Apple Products Could Allow for Arbitrary Code Execution

OVERVIEW

Multiple vulnerabilities have been discovered in Apple products, the most severe of which could allow for arbitrary code execution. Successful exploitation of the most severe of these vulnerabilities could allow for arbitrary code execution in the context of the logged on user. Depending on the privileges associated with the user, an attacker could then install programs; view, change, or delete data; or create new accounts with full user rights. Users whose accounts are configured to have fewer user rights on the system could be less impacted than those who operate with administrative user rights.

THREAT INTELLIGENCE

Apple is aware of a report that this issue may have been actively exploited against versions of iOS released before iOS 15.7. (CVE-2023-32434)

SYSTEMS AFFECTED:

- Versions prior to macOS Ventura 13.6.1
- Versions prior to macOS Sonoma 14.1
- Versions prior to macOS Monterey 12.7.1
- Versions prior to iOS 16.7.2 and iPadOS 16.7.2
- Versions prior to iOS 17.1 and iPadOS 17.1
- Versions prior tvOS 17.1
- Versions prior watchOS 10.1
- Versions prior Safari 17.1

RISK

Government:

- Large and medium government entities: **High**
- Small government entities: **Medium**

Businesses:

- Large and medium business entities: **High**
- Small business entities: **Medium**

Home users: Low

TECHNICAL SUMMARY

Multiple vulnerabilities have been discovered in Apple products, the most severe of which could allow for arbitrary code execution. Details of the vulnerabilities are as follows:

Tactic: *Execution* **(**TA0002**):**

Technique: *Exploitation for Client Execution* **(**T1203**):**

- A remote user may be able to cause unexpected app termination or arbitrary code execution. (CVE-2023-38403)
- An app may be able to execute arbitrary code with kernel privileges. (CVE-2023-40404, CVE-2023-40423, CVE-2023-42841, CVE-2023-32434, CVE-2023-32434)

- An attacker may be able to execute arbitrary code as root from the Lock Screen. (CVE-2023-41989)
- An attacker that has already achieved kernel code execution may be able to bypass kernel memory mitigations. (CVE-2023-42849)
- Parsing a file may lead to an unexpected app termination or arbitrary code execution. (CVE-2023-30774, CVE-2023-30774, CVE-2023-30774)
- Processing a file may lead to unexpected app termination or arbitrary code execution. (CVE-2023-42856)
- Processing malicious input may lead to code execution. (CVE-2023-4733, CVE-2023-4734, CVE-2023-4735, CVE-2023-4736, CVE-2023-4738, CVE-2023-4750, CVE-2023-4751, CVE-2023-4752, CVE-2023-4781)
- Processing web content may lead to arbitrary code execution. (CVE-2023-40447, CVE-2023-41976, CVE-2023-42852)

Additional lower severity vulnerabilities include:

- A device may be passively tracked by its Wi-Fi MAC address. (CVE-2023-42846)
- A device may persistently fail to lock. (CVE-2023-40445)
- A user's password may be read aloud by VoiceOver. (CVE-2023-32359)
- A website may be able to access sensitive user data when resolving symlinks. (CVE-2023-42844)
- A website may be able to access the microphone without the microphone use indicator being shown. (CVE-2023-41975)
- An app may be able to access protected user data. (CVE-2023-41077)
- An app may be able to access sensitive user data. (CVE-2023-40421, CVE-2023-41072, CVE-2023-41254, CVE-2023-42842, CVE-2023-42850, CVE-2023-42857, CVE-2023-40444)
- An app may be able to cause a denial-of-service to EndpointSecurity clients. (CVE-2023-42854)
- An app may be able to cause a denial-of-service. (CVE-2023-40449)
- An app may be able to read sensitive location information. (CVE-2023-40405, CVE-2023-40413)
- An app with root privileges may be able to access private information. (CVE-2023-40425)
- An attacker may be able to access passkeys without authentication. (CVE-2023-40401, CVE-2023-42847)
- An attacker with knowledge of a standard user's credentials can unlock another standard user's locked screen on the same Mac. (CVE-2023-42861)
- An attacker with physical access may be able to use Siri to access sensitive user data. (CVE-2023-41982, CVE-2023-41988, CVE-2023-41997)
- Hide My Email may be deactivated unexpectedly. (CVE-2023-40408)
- Photos in the Hidden Photos Album may be viewed without authentication. (CVE-2023-42845)
- Processing an image may result in disclosure of process memory. (CVE-2023-40416)
- Processing web content may lead to a denial-of-service. (CVE-2023-41983)
- Visiting a malicious website may lead to user interface spoofing. (CVE-2023-42438)
- Visiting a malicious website may reveal browsing history. (CVE-2023-41977)

Successful exploitation of the most severe of these vulnerabilities could allow for arbitrary code execution in the context of the logged-on user. Depending on the privileges associated with the user, an attacker could then install programs; view, change, or delete data; or create new accounts with full user rights. Users whose accounts are configured to have fewer user rights on the system could be less impacted than those who operate with administrative user rights.

RECOMMENDATIONS

We recommend the following actions be taken:

- Apply the stable channel update provided by Apple to vulnerable systems immediately after appropriate testing. (**M1051: Update Software**)
    - **Safeguard 7.1 : Establish and Maintain a Vulnerability Management Process:** Establish and maintain a documented vulnerability management process for enterprise assets. Review and update documentation annually, or when significant enterprise changes occur that could impact this Safeguard.
    - **Safeguard 7.2 : Establish and Maintain a Remediation Process:** Establish and maintain a risk-based remediation strategy documented in a remediation process, with monthly, or more frequent, reviews.
    - **Safeguard 7.6 : Perform Automated Vulnerability Scans of Externally-Exposed Enterprise Assets:** Perform automated vulnerability scans of externally-exposed enterprise assets using a SCAP-compliant vulnerability scanning tool. Perform scans on a monthly, or more frequent, basis.
    - **Safeguard 7.7 : Remediate Detected Vulnerabilities:** Remediate detected vulnerabilities in software through processes and tooling on a monthly, or more frequent, basis, based on the remediation process.
    - **Safeguard 16.13 Conduct Application Penetration Testing:** Conduct application penetration testing. For critical applications, authenticated penetration testing is better suited to finding business logic vulnerabilities than code scanning and automated security testing. Penetration testing relies on the skill of the tester to manually manipulate an application as an authenticated and unauthenticated user.
    - **Safeguard 18.1 : Establish and Maintain a Penetration Testing Program:** Establish and maintain a penetration testing program appropriate to the size, complexity, and maturity of the enterprise. Penetration testing program characteristics include scope, such as network, web application, Application Programming Interface (API), hosted services, and physical premise controls; frequency; limitations, such as acceptable hours, and excluded attack types; point of contact information; remediation, such as how findings will be routed internally; and retrospective requirements.
    - **Safeguard 18.2 : Perform Periodic External Penetration Tests:** Perform periodic external penetration tests based on program requirements, no less than annually. External penetration testing must include enterprise and environmental reconnaissance to detect exploitable information. Penetration testing requires specialized skills and experience and must be conducted through a qualified party. The testing may be clear box or opaque box.
    - **Safeguard 18.3 : Remediate Penetration Test Findings:** Remediate penetration test findings based on the enterprise's policy for remediation scope and prioritization.

- Apply the Principle of Least Privilege to all systems and services. Run all software as a non-privileged user (one without administrative privileges) to diminish the effects of a successful attack. (**M1026: Privileged Account Management**)
    - **Safeguard 4.7: Manage Default Accounts on Enterprise Assets and Software:** Manage default accounts on enterprise assets and software, such as root, administrator, and other pre-configured vendor accounts. Example implementations can include: disabling default accounts or making them unusable.
    - **Safeguard 5.4: Restrict Administrator Privileges to Dedicated Administrator Accounts:** Restrict administrator privileges to dedicated administrator accounts on enterprise assets. Conduct general computing activities, such as internet browsing, email, and productivity suite use, from the user's primary, non-privileged account.

- Restrict use of certain websites, block downloads/attachments, block Javascript, restrict browser extensions, etc. (**M1021: Restrict Web-Based Content**)

    - **Safeguard 2.3: Address Unauthorized Software:** Ensure that unauthorized software is either removed from use on enterprise assets or receives a documented exception. Review monthly, or more frequently.
    - **Safeguard 2.7: Allowlist Authorized Scripts:** Use technical controls, such as digital signatures and version control, to ensure that only authorized scripts, such as specific .ps1, .py, etc., files, are allowed to execute. Block unauthorized scripts from executing. Reassessbi-annually, or more frequently.
    - **Safeguard 9.3: Maintain and Enforce Network-Based URL Filters:** Enforce and update network-based URL filters to limit an enterprise asset from connecting to potentially malicious or unapproved websites. Example implementations include category-based filtering, reputation-based filtering, or through the use of block lists. Enforce filters for all enterprise assets.
    - **Safeguard 9.6: Block Unnecessary File Types:** Block unnecessary file types attempting to enter the enterprise's email gateway.

- Use capabilities to detect and block conditions that may lead to or be indicative of a software exploit occurring. **(M1050: Exploit Protection)**
    - **Safeguard 10.5: Enable Anti-Exploitation Features:** Enable anti-exploitation features on enterprise assets and software, where possible, such as Microsoft® Data Execution Prevention (DEP), Windows® Defender Exploit Guard (WDEG), or Apple® System Integrity Protection (SIP) and Gatekeeper™.

- Block execution of code on a system through application control, and/or script blocking. (**M1038: Execution Prevention**)
    - **Safeguard 2.5 : Allowlist Authorized Software:** Use technical controls, such as application allowlisting, to ensure that only authorized software can execute or be accessed. Reassess bi-annually, or more frequently.
    - **Safeguard 2.6 : Allowlist Authorized Libraries:** Use technical controls to ensure that only authorized software libraries, such as specific .dll, .ocx, .so, etc., files, are allowed to load into a system process. Block unauthorized libraries from loading into a system process. Reassess bi-annually, or more frequently.
    - **Safeguard 2.7 : Allowlist Authorized Scripts:** Use technical controls, such as digital signatures and version control, to ensure that only authorized scripts, such as specific .ps1, .py, etc., files, are allowed to execute. Block unauthorized scripts from executing. Reassess bi-annually, or more frequently.

- Use capabilities to prevent suspicious behavior patterns from occurring on endpoint systems. This could include suspicious process, file, API call, etc. behavior. (**M1040: Behavior Prevention on Endpoint**)
    - **Safeguard 13.2 : Deploy a Host-Based Intrusion Detection Solution**: Deploy a host-based intrusion detection solution on enterprise assets, where appropriate and/or supported.
    - **Safeguard 13.7 : Deploy a Host-Based Intrusion Prevention Solution:** Deploy a host-based intrusion prevention solution on enterprise assets, where appropriate and/or supported. Example implementations include use of an Endpoint Detection and Response (EDR) client or host-based IPS agent.

REFERENCES

Apple:

https://support.apple.com/en-us/HT213981

https://support.apple.com/en-us/HT213982

https://support.apple.com/en-us/HT213983
https://support.apple.com/en-us/HT213984
https://support.apple.com/en-us/HT213985
https://support.apple.com/en-us/HT213986
https://support.apple.com/en-us/HT213987
https://support.apple.com/en-us/HT213988
https://support.apple.com/en-us/HT213990

CVE:
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-4781
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-4752
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-4751
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-4750
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-4738
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-4736
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-4735
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-4734
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-4733
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-30774
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-32359
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-32434
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-38403
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-42861
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-42857
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-42856
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-42854
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-42852
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-42850
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-42849
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-42847
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-42846
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-42845
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-42844
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-42842
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-42841
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-42438
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-41997
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-41989
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-41988
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-41983
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-41982

http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-41977
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-41976
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-41975
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-41254
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-41077
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-41072
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-40449
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-40447
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-40445
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-40444
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-40425
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-40423
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-40421
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-40416
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-40413
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-40408
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-40405
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-40404
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-40401
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-40444