A Vulnerability in Apple Products Could Allow for Arbitrary Code Executio

Data: 2025-08-28 15:49:54

Autor: Inteligência Against Invaders

MS-ISAC ADVISORY NUMBER:

2025-075

DATE(S) ISSUED:

08/26/2025

OVERVIEW:

A vulnerability has been discovered in Apple products which could allow for arbitrary code execution. Successful exploitation 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 exploited in an extremely sophisticated attack against specific targeted individuals.

SYSTEMS AFFECTED:

- Versions prior to iOS 18.6.2 and iPadOS 18.6.2
- Versions prior to iPadOS 17.7.10
- Versions prior to macOS Sonoma 14.7.8
- Versions prior to macOS Sequoia 15.6.1
- Versions prior to macOS Ventura 13.7.8

RISK:

Government:

Large and medium government entitiesHIGH

Small governmentMEDIUM

Businesses:

Large and medium business entitiesHIGH

Small business entitiesMEDIUM

TECHNICAL SUMMARY:

A vulnerability has been discovered in Apple products which could allow for arbitrary code execution. Details of the vulnerability are as follows:

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

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

- An out-of-bounds write issue was addressed with improved bounds checking. Processing a malicious image file may result in memory corruption. (CVE-2025-43300)

Successful exploitation 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.