Office of Technology & Innovation

VULNERABILITY RATING // CRITICAL

NYC23-0188 APPLE ZERO-DAY MULTIPLE VULNERABILITIES

OTI PUBLISHED: 12/13/2023

MITIGATION

Agencies are advised to review the latest Apple security updates and apply the appropriate patches to all affected iOS, macOS, iPadOS devices. Apple has identified a total of 43 vulnerabilities including 2 Zero-Days.

All patches and workarounds should be tested before implementation in the production environment. Critical vulnerabilities are required to be patched within 7 days, High vulnerabilities are required to be patched within 30 days, as per the OTI Citywide policy for vulnerability mitigation standard (S-DE-CM-02).

IMPACT SUMMARY

The two Zero-Day vulnerabilities, (CVE-2023-42916) and (CVE-2023-42917), in the Webkit browser engine may disclose sensitive information. Multiple vulnerabilities affecting macOS Sonoma, (CVE-2023-42890), in the Webkit processing could lead to arbitrary code execution, (CVE-2023-42883), may lead to a denial-of-service (DoS) when processing an image and, (CVE-2023-42884), in the AVE Video Encoder app may be able to disclose kernel memory. Lastly, (CVE-2023-45866), could allow an attacker to inject keystrokes by spoofing a keyboard.

SOURCES + REFERENCES

https://support.apple.com/en-us/HT201222