Office of Technology & Innovation

VULNERABILITY RATING // HIGH

NYC23-0187 GOOGLE CHROME MULTIPLE VULNERABILITIES

OTI PUBLISHED: 12/13/2023

MITIGATION

Agencies are advised to update Google Chrome to the latest version, 120.0.6099.109 for Mac and Linux. Google has identified 5 High vulnerabilities.

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

Multiple High vulnerabilities identified in Chrome for Mac and Linux are, (CVE-2023-6702), Type Confusion in V8, (CVE-2023-6703), Use-after-free in Blink, (CVE-2023-6704), Use-after-free in libavif, (CVE-2023-6705), Use-after-free in WebRTC, and (CVE-2023-6706), Use-after-free in FedCM.

SOURCES + REFERENCES

https://chromereleases.googleblog.com/2023/12/stable-channel-update-for-desktop_12.html