Office of Technology & Innovation

VULNERABILITY RATING // HIGH

NYC23-0189 ZOOM MULTIPLE VULNERABILITIES

OTI PUBLISHED: 12/13/2023

MITIGATION

Agencies are advised to review the Zoom security updates and apply the appropriate patches to affected Zoom software. Zoom has identified two 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

A High path traversal vulnerability, (CVE-2023-43586), in Zoom Desktop Client for Windows, Zoom VDI Client for Windows, and Zoom SDKs for Windows, may allow an authenticated user to conduct an escalation of privilege (EoP). Another High improper access control vulnerability, (CVE-2023-43585), in Zoom Mobile App for iOS and Zoom Meeting SDKs for iOS and Android may allow an authenticated user to disclose the sensitive information via network access.

RESOURCES + REFERENCES

https://www.zoom.com/en/trust/security-bulletin/