Office of Technology & Innovation

VULNERABILITY RATING // CRITICAL

NYC23-0174 UBUNTU MULTIPLE VULNERABILITIES

OTI PUBLISHED: 11/22/2023

MITIGATION

Agencies are advised to review the Ubuntu security updates for the month of October, and apply the appropriate patches for all affected systems. Ubuntu identified 355 vulnerabilities, with 40 Critical and 175 High severity 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 Critical buffer overflow vulnerability in libqb library, (CVE-2023-39976), allows long log messages as the header size is not considered and could lead to a system crash. Other Critical vulnerabilities, (CVE-2023-40267), in GitPython before 3.1.32 could lead to remote code execution (RCE), (CVE-2023-38426) and (CVE-2023-38430), were discovered in SMB and could lead to an out-of-bounds read. Additionally, a Critical severity issue in ReadyMedia, (CVE-2023-33476), in versions from 1.1.15 up to 1.3.2 are vulnerable to buffer overflow.

SOURCES + REFERENCES

https://ubuntu.com/security/notices