Office of Technology & Innovation

VULNERABILITY RATING // CRITICAL

NYC23-0171 RED HAT MULTIPLE VULNERABILITIES

OTI PUBLISHED: 11/21/2023

MITIGATION

Agencies are advised to review the latest Red Hat security updates for the month of October and apply the appropriate patches to all affected systems. Red Hat has identified a total of 35 vulnerabilities including 6 Critical and 25 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 Critical vulnerability in Apache ZooKeeper, (CVE-2023-44981), allows for an authorization bypass via a user-controlled key. Another Critical vulnerability, (CVE-2023-46233), in crypto-js allows PBKDF2 to utilize SHA1, an unreliable cryptographic hash by default. Critical vulnerability, (CVE-2023-46604), was discovered in the OpenWire Module of Apache ActiveMQ and enables a remote user to execute arbitrary shell commands. There is a Critical vulnerability, (CVE-2023-5730), affecting Firefox 118, Firefox ESR 115.3, and Thunderbird 115.3 that could lead to an attacker running arbitrary code. Another Critical vulnerability, (CVE-2023-39332), in the Various node:fs function allows path traversal. Redhat has also addressed multiple High vulnerabilities that lead to escalation of privilege (EoP), buffer overflow, remote code execution (RCE), authentication bypass, and denial of service (DoS).

SOURCES + REFERENCES

https://access.redhat.com/security/security-updates/#/cve