Office of Technology & Innovation

VULNERABILITY RATING // CRITICAL

NYC23-0175 SUSE MULTIPLE VULNERABILITIES

OTI PUBLISHED: 11/22/2023

MITIGATION

Agencies are advised to review the latest SUSE security updates for the month of October and apply the appropriate patches to all affected devices. SUSE has identified a total of 274 vulnerabilities including 23 Critical and 127 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, (CVE-2023-42464), in Spotlight RPC methods allows a malicious actor to potentially gain complete control and execute remote code (RCE) on affected systems. Another Critical buffer overflow vulnerability, (CVE-2020-22217), in c-ares before 1_16_1 thru 1_17_0 can result in a system crash. Additionally, the Critical vulnerabilities, (CVE-2023-41360), in FRRouting can lead to information disclosure, (CVE-2023-3824), in PHP can allow for a stack buffer overflow and possible memory corruption and, (CVE-2023-40397, CVE-2023-5176, CVE-2023-0687), causes memory corruption leading to buffer overflow.

SOURCES + REFERENCES

https://www.suse.com/support/update/