Overall Rating - Critical

BRITISH COLUMBIA

This notification is intended as an informational bulletin for technical audiences.

Summary

The Vulnerability and Risk Management (VRM) Team is aware of multiple vulnerabilities recently disclosed in Python through 3.9.1.

Technical Details

- An XML External Entity (XXE) issue was discovered in Python through 3.9.1. The plistlib module no longer accepts entity declarations in XML plist files to avoid XML vulnerabilities. CVE-2022-48565
- An issue was discovered in compare_digest in Lib/hmac.py in Python through 3.9.1. Constant-time-defeating optimisations were possible in the accumulator variable in hmac.compare_ digest. CVE-2022-48566
- A use-after-free exists in Python through 3.9 via heappushpop in heapq. CVE-2022-48560

These vulnerabilities are rated as an overall **Critical** Severity.

Recommended Action

- Investigate how your area of responsibility is affected.
- Notify business owner(s) as required.
- Ensure mitigation is performed as soon as possible.

Please notify VRM with any questions or concerns you may have.

References

- CVE-2022-48565, CVE-2022-48566, CVE-2022-48560
- https://bugs.python.org/issue42051
- https://lists.debian.org/debian-lts-announce/2023/09/msg00022.html
- https://bugs.python.org/issue40791
- https://bugs.python.org/issue39421
- https://lists.debian.org/debian-lts-announce/2023/09/msg00022.html