Overall rating: High

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

Summary

The Vulnerability and Risk Management (VRM) Team is aware of two recently disclosed vulnerabilities in Trellix Enterprise Security Manager. Affects versions 11.6.3 and earlier

Technical Details

- An OS common injection vulnerability exists in the ESM certificate API, whereby incorrectly neutralized special elements may have allowed an unauthorized user to execute system command injection for the purpose of privilege escalation or to execute arbitrary commands. CVE-2023-3313

- A vulnerability arises out of a failure to comprehensively sanitize the processing of a zip file(s). Incomplete neutralization of external commands used to control the process execution of the .zip application allows an authorized user to obtain control of the .zip application to execute arbitrary commands or obtain elevation of system privileges. CVE-2023-3314

These vulnerabilities are rated as a **High** Severity.

Recommended Action

- Investigate how your area of responsibility is affected.
- Notify business owner(s) as required.
- *Ensure mitigation is performed at your next change window.*

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

References

- CVE-2023-3313, CVE-2023-3314
- https://kcm.trellix.com/corporate/index?page=content&id=KB56057
- Trellix Security Advisory (SB10403)
- Trellix Security Advisories