November 30, 2023

Overall Rating - High

BRITISH COLUMBIA

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

Summary

The Vulnerability and Risk Management (VRM) Team is aware Trellix published security advisories to address vulnerabilities in the following products:

- Trellix Application and Change Control (TACC) – versions prior to 8.4.0
- Trellix Enterprise Security Manager (ESM) – versions prior to 11.6.9

Technical Details

he TACC ePO extension offers the ability for an authorised administrator to access the "Inventory" section of the ePO extension and upload custom GTI ratings through the **Import GTI ratings** option. There's an error in the parsing logic, which allows a zip file to be uploaded that utilizes path traversal in the archive file paths to trigger remote code execution on the ePO server. This is only applicable to on-premises ePO servers.

The risk of exploitation can be reduced by limiting access to the ePO interface through network access controls, restricting the number of users, and granting only the required level of access to perform the required tasks. It's recommended that the interface for your ePO server isn't placed on the internet, allowing only access from trusted networks.

These vulnerabilities are rated as an overall **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-2023-5607
- Trellix Security Advisory (SB10411)
- Trellix Security Advisory (SB10413)
- Trellix Security Advisories

Please note that we will be transitioning to a new site on August 31, 2023, where we will post the vulnerability reports.

You will be able to find all the reports that we have published as well as all future reports here: Cybersecurity Alerts