January 22, 2024

ADO Action Required: Trend Micro Endpoint Agents Upgrade

On January 2, 2024, Trend Micro published an advisory stating that **all Trend Micro Deep Security Linux agents must be upgraded to version 20.0.0-7943 or higher before February 4, 2024.** The Enterprise Shared Services (ESS) Security team has determined that the newer version is critical to maintaining a strong security posture.

All teams using Linux Deep Security agents are affected and must take action to prevent the loss of endpoint protection and kernel support.

Impact

After February 4, 2024, in addition to the Center for Clinical Standards and Quality (CCSQ) losing the ability to properly maintain and enforce Trend Micro monitoring and configurations within our environment, application teams may experience the following outcomes without the upgrade:

- New endpoint threats will not be detected due to incompatibility between the Trend Micro agent and your kernel.
- Systems may experience instability if the Trend Micro agent is incompatible with your kernel version.
- Systems will be at risk of outages or security compromises of data stored/processed by those systems.
- Authority to Operate (ATO) may be impacted due to the inability to inherit security controls (e.g., SI-2, RA-5) due to the lack of compliant system components (agents).

Timeline

January 2, 2024	Trend Micro published an advisory to upgrade all Trend Micro Deep Security Linux agents to version 20.0.0-7943 or higher before February 4th.
January 22, 2024 - February 4, 2024	Application Development Organizations (ADOs) are to upgrade their agents using one of the upgrade options below.

By February 4, 2024	All affected customers should be upgraded to version 20.0.0-7943 or higher.

Upgrade Options

Please complete one of the below upgrade options:

1. Consume the Gold Image released on **January 18, 2024** (recommended).
2. Use the upgrade script found for either Amazon Linux 2 or RHEL OS. Instructions and files to be executed by the ADOs can be found in Confluence.

Questions

We look forward to working with you and your team. Reach out in the #help-devsecops Slack channel if you have any questions.

If you need additional information, please work with your assigned CMS Information System Security Officer (ISSO) (List here), the CCOM Security Analyst team, or reach out on QualityNet Slack: #qnet-security-community.

Join the QualityNet Mailer List:
QNet Security Communications