Illumio® Core C-VEN

Version: 21.2.1

Release Notes

06/25/2021

19000-100-21.2.1

Contents

Welcome

These release notes describe the resolved issues and known issues for the Illumio Containerized VEN 21.2 release.

Document Last Revised: June 2021
Document ID: 19000-100-21.2.1

> ⓘ Containerized VEN issues have been moved to this document from “Illumio Core Release Notes 21.2.”

What's New in This Release

To learn what's new and changed in 21.2.1, see What's New in This Release on the Illumio Technical Information portal.

> ⚠ The Illumio Core platform was previously known as the Illumio Adaptive Security Platform (ASP). References to "Adaptive Security Platform" and ASP still appear in these release notes.

Security Information

For information about security issues, security advisories, and other security guidance pertaining to this release, see Illumio’s Knowledge Base in Illumio's Support portal.

Product Version

Current PCE Version: 21.2.1 (LTS candidate)
Current VEN Version: 21.2.1 (LTS candidate)

Standard versus LTS Releases

21.2.1-PCE is a Long Term Support (LTS) candidate release.
21.2.1-VEN is a Long Term Support (LTS) candidate release.
For information on Illumio software support for Standard and LTS releases, see Versions and Releases on the Illumio Support portal.

Release Types and Numbering

Illumio ASP release numbering uses the following format: “a.b.c-d+e”

- “a.b”: Standard or LTS release number, for example, “21.2”
- “.c”: Maintenance release number, for example, “.1”
- “-d”: Optional descriptor for pre-release versions, for example, “preview2”
- “+e”: Hot Fix release descriptor, for example, “+H1”, “+H2”, “+H3”.

Resolved Issue in 21.2.1

- Illumio detected a vulnerability in the Containerize VEN (C-VEN) image for 21.2.0. The vulnerability is described in the *RHSA-2021:1469 - Security Advisory* (https://access.redhat.com/errata/RHSA-2021:1469).
  In the C-VEN 21.2.0 release, the Illumio C-VEN container image used a lightweight version of RHEL 7.8. The bind package in the image was affected by this vulnerability. For information about the bind issue, see *CVE-2021-25215* (https://access.redhat.com/security/cve/CVE-2021-25215) in the Red Hat Customer Portal.
  Red Hat has evaluated the severity of this issue to be in the high severity range with a maximum CVSSv3 base score of 7.5.
  In C-VEN 21.2.1, Illumio has resolved this issue by updating the C-VEN base OS image to RHEL 7.9 to address this vulnerability. We will strongly encourage our customers to upgrade to the new image in the C-VEN 21.2.1 release.

Known Issues in 21.2.1

- **Platform logs on IKS display a failed to load policy error** (E-79515)
  When the PCE and C-VEN experience connectivity issues or increased network latency occurs between them, you can experience a delay in the PCE applying policy to host workloads. The PCE will apply the policy updates as soon as the connection issues between the PCE and C-VEN correct themselves. However, it can take up to 5 minutes for the C-VEN to heartbeat with the PCE and apply the policy. Illumio recommends that you maintain a good connection

state between the PCE and the C-VENs running on your host workloads to avoid unexpected delays in policy propagation.

- **Unexpected tampering events can occur** (E-79445)
  You might see occasional firewall tampering events even when the Firewall Co-Existence option is enabled in the PCE for the container and host workloads in a container cluster. This issue can occur when Illumio Kubelink can't connect to the PCE and, as a result, the container cluster is not "In Sync."
- **Some pods aren't set to ready within the ready timer of the Readiness Gate** (E-79378)
  When the PCE and C-VEN experience connectivity issues or increased network latency occurs between them, applying settings to the Illumio Policy Readiness Gate on the pods can be delayed. This delay occurs due to a delay in policy sync. The PCE will apply the settings to the Readiness Gate as soon as the connection issues between the PCE and C-VEN correct themselves. However, it can take up to 5 minutes for the C-VEN to heartbeat with the PCE and for the PCE to apply the settings to the Readiness Gate. Illumio recommends that you maintain a good connection state between the PCE and the C-VENs running on your host workloads to avoid this delay.
- **IKS VPN Pod traffic not showing in Illumination/Explorer** (E-71163)
  You might not see long-lived flows that were established before the firewall is programmed for container workloads (this does not apply to host workloads). There is no workaround because it's a feature that has not yet been implemented for container workloads and not an issue.
- **The outbound rule opens up both TCP and UDP ports** (E-60837)
  When a Kubernetes service has both port 1234/TCP and port 2345/UDP configured, a rule configured with the pod as Consumer and Virtual Service as Provider will open up both ports 1234/TCP and 2345/TCP as well as 1234/UDP and 2345/UDP on the pod's firewall (outbound rule). This configuration is supported with Illumio ASP. In this case, only the port number associated with the port statement will show this issue, the port number associated with the targetPort statement will not show this issue and will attach to the protocol specified in the Service YAML file. For more information and an example, see Illumio Core for Kubernetes and OpenShift .