TECHNICAL
DOCUMENTATION

Illumio Advisories

Table of Contents

Product Advisories

Review these Illumio product advisories.

- Missing Node Annotation in OpenShift 4.19 [4]: Published October 8, 2025
- Upcoming Changes to TLS Certificate Requirements [4]: Published September 10, 2025
- Bitnami Repository Changes [6]: Published August 22, 2025

Missing Node Annotation in OpenShift 4.19

In OpenShift 4.19, the node annotation `k8s.ovn.org/node-gateway-router-lrp-ifaddrs` is missing. This omission impacts the functionality of virtual services such as LoadBalancer and NodePort within CLAS environments.

As a result, customers must manually create an additional infrastructure rule in the PCE to maintain proper communication and ensure service availability.

Add the following rule to the PCE:

```
Source: IP List = 100.64.0.0/16
Destination: All Pods (Label: all_pods_label)
Destination Services: All Services
```

Upcoming Changes to TLS Certificate Requirements

Date of Product Advisory Announcement: September 2025

Starting October 1, 2025, public certificate authorities (CAs), including DigiCert, will stop issuing public TLS certificates that include the Client Authentication (Client Auth) Extended Key Usage (EKU) by default. Customers must explicitly request this extension when generating certificates intended for use with Illumio software. On or around May 1, 2026, DigiCert and other public certificate authorities (CAs) will fully prevent the option to choose the Client Authentication EKU during enrollment for public TLS certificates.

Following this change, starting on June 15, 2026, Google Chrome and other browsers will stop trusting any newly issued server certificates that include the Client Auth EKU. This industry-wide change can affect how TLS certificates are used in secure environments that depend on the Client Auth EKU.

Audience

This change applies to on-premises customers only.

Impact to On-Premises Policy Compute Engine (PCE)

Illumio PCE currently requires TLS certificates with the Client Auth EKU for some internal services. Using certificates without this EKU may prevent key services from starting or operating correctly. Until a product update is available to address this change, customers are advised to continue issuing certificates with the Client Auth EKU to avoid operational disruptions.

Impact to Network Enforcement Node (NEN)

The Network Enforcement Node (NEN) also relies on TLS certificates with the Client Auth EKU for some internal services. Certificates issued without this EKU may result in operational disruptions. Customers should make sure that certificates used with NEN deployments include the Client Auth EKU until a product update is available.

Recommended Action

- Continue to generate TLS certificates that include the Client Auth EKU to ensure uninterrupted functionality of Illumio PCE services.
- If you're using a public certificate authority such as DigiCert, you must explicitly request the inclusion of the Client Auth EKU when you generate certificates.

Planned Illumio Response

Product updates will be made available for the PCE and NEN that will support this industry-wide transition.

Frequently Asked Questions (FAQs)

Review these FAQs if you need more information.

What is changing on October 1, 2025?

DigiCert and other major certificate authorities will stop issuing TLS certificates with the Client Auth EKU by default. Customers who require this extension for mutual TLS must request it explicitly.

What is changing on May 1, 2026?

Google Chrome will stop trusting server certificates that include the Client Auth EKU if they are issued after this date. As a result, users may encounter browser warnings or errors when accessing the PCE web UI using such certificates.

Why does Illumio PCE require the Client Auth EKU today?

The Client Auth EKU is required for inter-node communication between PCE nodes.

Why does NEN require the Client Auth EKU today?

TLS certificates with the Client Auth EKU are used to secure some internal services within the NEN.

Can we use separate certificates for internal and external services?

Currently, Illumio supports a single certificate model. Using separate certificates for internal and browser-facing services is not supported.

What if we use public certificates from providers like DigiCert?

You can continue using public CAs for now, but after October 1, 2025, you must explicitly request the Client Auth EKU.

What happens if we don't make any changes?

If certificates without the Client Auth EKU are used, some services in PCE or NEN may fail to start or operate correctly. In addition, Chrome may block access to web interfaces using certificates that include the EKU after June 15, 2026.

Will this impact SaaS deployments?

This advisory specifically applies to on-premises PCE and NEN deployments.

What changes are coming from Illumio?

Illumio plans to make product updates available that align with the industry-wide transition.

Where can we find more information about this industry-wide change?

- SSL.com article
- Chrome advisory
- DigiCert update

Bitnami Repository Changes

Bitnami is implementing a significant change to its container image distribution model, effective August 28, 2025.

As a result of this change, the Bitnami etcd image used in the Illumio Container CLAS Storage will be migrating.

Who is Impacted

Customers with CLAS enabled who use the default Helm chart values from quay.io Illumio Kubernetes Operator or pull images directly from the public Bitnami Docker repository.

Who is Not Impacted

- Customers with CLAS deployments that pull images from a private repository.
- Customers running the product in a Legacy (Non-CLAS) deployment.

Impact

- If you do not take any action before the repository migration, any restart of the Illumio storage pod will fail. This will result in policy update failures in your Kubernetes and OpenShift clusters.
- If the repository is not updated, existing CLAS deployments will continue to run but will fail when the storage pod is restarted and rescheduled on a different Kubernetes node.

Required Action

IMPORTANT

To ensure uninterrupted operation of your applications and Illumio policy in your clusters, you must update your Helm chart yaml values file before August 28, 2025.

Instructions to update the etcd Repository for CLAS Deployment

1. Add or update the following section of your helm chart values file:

```
storage:
  registry: "docker.io/bitnamilegacy"
```

2. Get the current version of the helm chart:

```
helm list --namespace illumio-system
```

3. Use the same version of the helm upgrade:

```
helm upgrade illumio -f illumio-values.yaml oci://quay.io/illumio/
illumio --namespace illumio-system --version VERSION_FROM_ABOVE
```

4. Confirm that the storage pod is running:

```
kubectl get pod --namespace illumio-system
```

5. Confirm that the etcd image repo is updated:

```
kubectl get statefulset --namespace illumio-system illumio-storage --
output yaml|grep image:
```

6. Confirm that etcd is initialized. One of the last few lines of the storage pod log will say successfully notified init daemon:

```
kubectl logs --namespace illumio-system statefulset/illumio-storage
```

7. Confirm that kubelink has restarted and is running:

```
kubectl get pod --namespace illumio-system
```

8. Confirm that kubelink policy fetches and updates:

```
kubectl logs --namespace illumio-system deployment/illumio-kubelink
```

9. Confirm the etcd database size:

```
kubectl exec --namespace illumio-system illumio-storage-0 -- etcdctl
endpoint status --write-out=table
```

Recommendation

To ensure continuity and uninterrupted service, Illumio recommends that you review and consider upgrading to the new 5.6 version of the Illumio Kubernetes Operator.

Security Advisories

Illumio provides information about Common Vulnerabilities and Exposures (CVE) that applies to its products. CVE is a glossary that classifies vulnerabilities. The glossary analyzes vulnerabilities and then uses the Common Vulnerability Scoring System (CVSS) to evaluate the threat level of a vulnerability.

IMPORTANT

Monitor this section for new information about security advisories. The content in this section is organized by month and year, and is updated on a regular basis.

March 2025 Security Advisories

Here's a list of the security advisories for 2025.

Ruby SAML Gem Component Authentication Bypass Vulnerability

The Ruby SAML gem is affected by an authentication bypass vulnerability. This impacts the Illumio PCE in both SaaS and on-premises deployments. An authenticated attacker could potentially leverage this vulnerability to authenticate as another SAML user.

For SaaS customers, the target user could be in a different organization and on a different cluster.

IMPORTANT

No action is required for SaaS PCE customers.

Severity

High: CVSS score is 8.8

CVSS: AV:N/AC:L/AT:N/PR:N/UI:N/VC:H/VI:H/VA:N/SC:N/SI:N/SA:N/E:P

Affected Products and Patch Information

Security vulnerabilities addressed by this Security Alert affect the products listed below.

Table 1. Products Affected by the Security Vulnerability

Affected Products	Affected Versions	Fixed Version
Illumio Core PCE	24.2.20	24.2.21
	23.5.31	23.5.32
	23.2.31	23.2.32
	22.5.34	22.5.35
	22.2.43	22.2.44

Resolution

Upgrade to the latest release for a given major version.

References

- https://nvd.nist.gov/vuln/detail/CVE-2025-25291
- https://nvd.nist.gov/vuln/detail/CVE-2025-25292
- https://nvd.nist.gov/vuln/detail/CVE-2025-25293
- Github Summary

Skipped Critical Patch Updates

Illumio strongly recommends that you apply the security patches as soon as possible. If you skipped one or more Critical Patch Updates and are concerned about products that do not have security patches announced in this update, review the previous advisories to determine appropriate actions.

Frequently Asked Questions

- What software components are affected?
  Only the Illumio PCE is impacted by this vulnerability.
- Is Core SaaS affected?
  SaaS PCE clusters were impacted. Those environments have been patched.
- I'm using CloudSecure. Am I impacted?
  The CloudSecure platform is not affected.
- Will the patch affect performance?
  The update is not expected to affect performance.
- Has Illumio investigated if this vulnerability was used on any SaaS PCEs?

Illumio is currently investigating all available data from the production SaaS environment and has so far found no indications that the issue has been exploited.

- I can't apply the patch immediately. How can I mitigate the issue in the meantime?

  This vulnerability requires SAML to be enabled on the customers PCE in order to be exploited. Customers who cannot patch their PCEs immediately, and who wish to mitigate this issue, can choose to disable SAML authentication on their PCE. For details see the "Authentication" topic in the PCE Administration Guide.
  - Additionally, customers can Enable Source IP restrictions to limit access to trusted source IPs (for example, for privileged accounts). See the topic "Configure Access Restrictions and Trusted Proxy IPs" in the PCE Administration Guide.
- How long will the upgrade take?

  The fix will be provided in a normal code release so this will take the same amount of time as any PCE upgrade.
- Were any Illumio customers impacted by this vulnerability?

  Illumio is not aware of any exploitation of this vulnerability within any customer environments.

Modification History

- March, 2025: Initial Publication of CVE

September 2024 Security Advisories

Here's a list of the security advisories for 2024.

Ruby SAML gem component authentication bypass vulnerability

The Ruby SAML gem is affected by an authentication bypass vulnerability, which impacts the Illumio PCE in both SaaS and on-premises deployments. An authenticated attacker could potentially leverage this vulnerability to authenticate as another SAML user. For SaaS customers, the target user can be in a different org and on a different cluster.

Severity

Critical: CVSS score is 9.9

CVSS: AV:N/AC:L/PR:L/UI:N/S:C/C:H/I:H/A:H

Affected Products and Patch Information

Security vulnerabilities addressed by this Security Alert affect the products listed below.

Table 2. Products Affected by the Security Vulnerability

Affected Products	Affected Versions	Fixed Version
Illumio Core PCE	<= 21.5.36	>= 21.5.37
	<= 22.2.42	>= 22.2.43
	<= 22.5.32	>= 22.5.34
	<= 23.2.30	>= 23.2.31
	<= 23.5.21	>= 23.5.22
	<= 24.2.0	>= 24.2.10

Resolution

Upgrade to the latest release for a given major version.

References

- https://nvd.nist.gov/vuln/detail/CVE-2024-45409
- https://github.com/advisories/GHSA-jw9c-mfg7-9rx2

Skipped Critical Patch Updates

Illumio strongly recommends that customers apply security patches as soon as possible. For customers that have skipped one or more Critical Patch Updates and are concerned about products that do not have security patches announced in this Critical Patch Update, please review previous Critical Patch Update advisories to determine appropriate actions.

Discovered By

External Security Firm

Frequently Asked Questions

- What software components are affected?
  Only the Illumio PCE is impacted by this vulnerability.
- What products did this affect?
  This vulnerability impacts the PCE, including Core on-premises deployments, Core SaaS, Endpoint, MSP, and Edge.
- Is Core SaaS affected?
  SaaS PCE clusters were impacted. Those environments have been patched.
- I'm using Cloud. Am I impacted?
  The Cloud platform is not affected.

- Will the patch affect performance?

  The update is not expected to affect performance.
- How can I tell if this vulnerability was used against my on-premises PCE?

  Illumio is creating queries that can be used by customers to detect known vectors for exploitation of this vulnerability. Please contact Illumio Support or your account team for assistance. If you suspect this vulnerability was used within your environment, please reach out to Illumio Support.
- Has Illumio investigated if this vulnerability was used on any SaaS PCEs?

  Illumio is currently investigating all available data from the production SaaS environment and has so far found no indications that the issue has been exploited.
- I can't apply the patch immediately. How can I mitigate the issue in the meantime?

  This vulnerability requires SAML to be enabled on the customer's PCE in order to be exploited. Customers who cannot patch their PCEs immediately, and who wish to mitigate this issue, can choose to disable SAML authentication on the PCE. For details, see the "Authentication" topic in the PCE Administration Guide. Additionally, customers can enable IP restrictions to limit access to only trusted source IPs (for example, for privileged accounts). For details, see the "Configure Access Restrictions and Trusted Proxy IPs" topic in the .
- How long will the upgrade take?

  The fix will be provided in a normal code release so this will take the same amount of time as any PCE upgrade.
- Were any Illumio customers impacted by this vulnerability?

  Illumio is not aware of any exploitation of this vulnerability within any customer environments.

Modification History

- September, 2024: Initial Publication of CVE

September 2023 Security Advisories

Here's a list of the security advisories for 2023.

Authenticated RCE due to unsafe JSON deserialization

Unsafe deserialization of untrusted JSON allows execution of arbitrary code on affected releases of the Illumio PCE. Authentication to the API is required to exploit this vulnerability. The flaw exists within the network_traffic API endpoint. An attacker can leverage this vulnerability to execute code in the context of the PCE's operating system user.

Severity

Critical: CVSS score is 9.9

CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:C/C:H/I:H/A:H

Affected Products and Patch Information

Security vulnerabilities addressed by this Security Alert affect the products listed below.

Table 3. Products Affected by the Security Vulnerability

Affected Products	Affected Versions	Fixed Version
Illumio Core PCE	<= 19.3.6	>= 19.3.7
	<= 21.2.7	>= 21.2.8
	<= 21.5.35	>= 21.5.36
	<= 22.2.41	>= 22.2.42
	<= 22.5.30	>= 22.5.31
	<= 23.2.10	>= 23.2.11

Resolution

Upgrade to the latest release for a given major version.

References

https://www.cve.org/CVERecord?id=CVE-2023-5183

Skipped Critical Patch Updates

Illumio strongly recommends that customers apply security patches as soon as possible. For customers that have skipped one or more Critical Patch Updates and are concerned about products that do not have security patches announced in this Critical Patch Update, please review previous Critical Patch Update advisories to determine appropriate actions.

Discovered By

External Security Firm

Frequently Asked Questions

- What software components are affected?
  Only the Illumio PCE is impacted by this vulnerability.
- What products did this affect?
  This vulnerability impacts the PCE, including Core on-premises deployments, Core SaaS, Endpoint, MSP, and Edge.
- Is Core SaaS affected?

SaaS PCE clusters were impacted. Those environments have been patched.

- I'm using Cloud. Am I impacted?

  The Cloud platform is not affected.
- How can I tell if this vulnerability was used against my on-premises PCE?

  Illumio is creating queries that can be used by customers to detect known vectors for exploitation of this vulnerability. Please contact Illumio Support or your account team for assistance. If you suspect this vulnerability was used within your environment, please reach out to Illumio Support.
- Has Illumio investigated if this vulnerability was used on any SaaS PCEs?

  Illumio is currently investigating all available data from the production SaaS environment and has so far found no indications that the issue has been exploited.
- I can't apply the patch immediately. How can I mitigate the issue in the meantime?

  This vulnerability requires SAML to be enabled on the customer's PCE in order to be exploited. Customers who cannot patch their PCEs immediately, and who wish to mitigate this issue, can choose to disable SAML authentication on the PCE.
- Reference

  For details, see the topic Authentication in the PCE Administration Guide.

  Additionally, customers can: Enable IP restrictions to limit access to only trusted source IPs (for example, for privileged accounts). For details, see the topic Configure Access Restrictions and Trusted Proxy IPs in the PCE Administration Guide.
- How long will the upgrade take?

  The fix will be provided in a normal code release so this will take the same amount of time as any PCE upgrade.
- Were any Illumio customers impacted by this vulnerability?

  Illumio is not aware of any exploitation of this vulnerability on any customer environments.