Security Advisory: FlexNet Beacon Security Update (CVE-2026-110390)

CVE-2026-110390 (https://www.cve.org/CVERecord?id=CVE-2026-110390)

CVSS 4.0 Score: 6.9 (Medium)

CVSS 4.0 Metric:
CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:N/VC:L/VI:N/VA:N/SC:N/SI:N/SA:N

Affected Component: FlexNet Beacon

Summary

Flexera has identified a security vulnerability affecting certain FlexNet Beacon deployments. Under specific configurations, Beacon services may permit unauthenticated access to information that was not intended to be publicly available.

While the issue does not provide direct access to customer business data, it may expose infrastructure configuration information that could be leveraged as part of broader reconnaissance activities.

Flexera has released remediation updates and strongly recommends that all customers review their environments and apply the corrective actions described below as soon as possible.

Who Is Affected

The issue affects Inventory Beacon deployments used with Flexera One IT Asset Management, FlexNet Manager Suite, and Flexera One IT Visibility where Beacon web services allow anonymous (unauthenticated) access. Anonymous access is the default configuration.

- Flexera One IT Asset Management and FlexNet Manager Suite: Beacon policy information, including discovery and inventory targeting details, may be accessible without authentication.
- Flexera One IT Visibility: Beacon targeting information may be accessible without authentication.

Customers who have configured authentication on all Beacon web services may have reduced exposure but should still apply the updates described below.

Recommended Actions

1. Apply the Latest Beacon Update Immediately

Customers should upgrade to the latest Beacon release or hotfix package provided by Flexera.

Applying the update addresses the primary exposure identified by Flexera's investigation.

Refer to the following page for detailed instructions: FlexNet Beacon security hotfix IOK-2107311 (https://community.flexera.com/s/article/Flexera-Beacon-security-hotfix-IOK-2107311)

2. Review Beacon Configuration Against Security Best Practices

Flexera strongly recommends that customers review Beacon configuration against security best practices.

The following product documentation contains a list of recommendations for improving the security of your Beacons: Beacon Security Best Practices (https://docs.flexera.com/flexera-one/it-assets/inventory-beacon-overview/fib-ref-introduction/best-practices-for-inventory-beacon).

Following these recommendations does not guarantee freedom from security issues, but they can significantly reduce your risk.

Risk Description

The issue may allow exposure of infrastructure-related configuration information under certain deployment scenarios.

Flexera Actions

Flexera has:

- Investigated and validated the issue.
- Developed and released corrective software updates.
- Reviewed related Beacon functionality for similar exposure paths.
- Published mitigation guidance.
- Continued monitoring for indications of misuse or exploitation.

Additional Guidance

Customers with heightened security requirements or internet-facing Beacon deployments should prioritize remediation activities and review Beacon deployment configurations against their organization's standard IIS hardening practices.

Customers requiring assistance should contact Flexera Support.

Document history

2026-11-04 13:01 UTC: Initial version published.

SUBSCRIBE

FlexNet Manager Suite On-Premises | Flexera One

Product: Flexera One
Solution Area: IT Asset Management
Also Applies To: FlexNet Manager Suite
Deployment type: Cloud;On-premises
Visibility: Guest
URL Name: Flexera-Beacon-Security-Advisory-CVE-2026-110390

Was this helpful?

YES NO

Files (0) (/s/relatedlist/ka6PL000004wCL3YAM/AttachedContentDocuments)

© 2026 Flexera. All rights reserved.