

FlexNet Publisher 2026 R1 (11.19.10) Vulnerability Assessment

March 2026
Revision 00

Introduction	2
Necessity of CVE in Vulnerability Assessment.....	2
Revenera's Score Assessment	2
Boost.....	2
Revenera Score	3
Vulnerabilities	3
Best Practices	3
CryptoPP	3
Vulnerabilities	3
Legal Information	5

Introduction

This document provides an overview of the vulnerabilities identified in third-party components used within FlexNet Publisher, along with Revenera's assessment of their relevance and impact. It explains the importance of CVE-based reporting, Revenera's scoring methodology, and summarizes the security posture of FlexNet Publisher with respect to third-party components or libraries.

- [Necessity of CVE in Vulnerability Assessment](#)
- [Revenera's Score Assessment](#)
- [Boost](#)
- [CryptoPP](#)

Necessity of CVE in Vulnerability Assessment

Revenera recommends providing additional information on vulnerabilities which are detected in the field such as CVEs (Common Vulnerabilities and Exposures). Details on the vulnerability, including the lines of code that are vulnerable and the attack method, will help Revenera team to thoroughly analyze and resolve the issue. Generally, a CWE (Common Weakness Enumeration) has insufficient data to resolve the vulnerability.



Note • The CWE (Common Weakness Enumeration) complements the CVE (Common Vulnerabilities and Exposures) via focusing on the types of weaknesses or vulnerabilities that may exist in software. The CVE displays specific instances of vulnerabilities and the CWE categorizes common flaws or weaknesses that may lead to vulnerabilities.

Revenera's Score Assessment

The Revenera team has performed the assessment with consideration of how FlexNet Publisher is deployed and used by customers.

Boost

FlexNet Publisher currently utilizes Boost version 1.56. Many producers have inquired about the use of this older Boost version in the software. Revenera clarifies that Boost does not have an official End-of-Life (EOL) policy. While FlexNet Publisher has attempted to upgrade to later versions of Boost, these efforts have led to issues with the overall build system, causing the software to function improperly. As of now, 1.56 remains the last stable version of the Boost that ensures FlexNet Publisher operates without significant impact on product functionality.

Reverera Score

Overall CVSS 3.1 score is 3.0, categorizing it as low severity. For more details, please refer to the [National Vulnerability Database](#).

Vulnerabilities

The following vulnerabilities are detected in the Boost software:

- **Vulnerability ID: BDSA-2018-2656**—The BDSA-2018-2656 vulnerability exists in Boost's `basic_regex_creator` function, which causes a buffer over-read, leading to a denial-of-service. However, FlexNet Publisher is not vulnerable since it does not rely on regex. Additionally, regex dependencies have been removed from FlexNet Publisher 11.19.8 onwards. Despite this remediation, black duck and other scans could flag this up because they may not perform a deep scan and flag up things purely based on boost version.
- **Vulnerability ID: BDSA-2018-1263**—Boost incorrectly casts from `"boost::detail::shared_count::shared_count"` to `"boost::detail::sp_counted_base"`, causing type confusion leading to a denial-of-service. FlexNet Publisher utilizes Boost's `SharedPtr` library. Reverera has been unable to find any information on this vulnerability in the Boost community, vulnerability calculators, or NVD searches. Additionally, an internal tool, FlexNet Code Insight, which leverages the NVD knowledge base, is unable to flag this vulnerability. Given the limited available information, we assessed the vulnerability and determined that its severity is low. However, Reverera prioritizes addressing Common Vulnerabilities and Exposures (CVEs) over Common Weakness Enumerations (CWEs).

Best Practices

For a best practice, product producers must ensure that their customers adhere to the following guidelines:

- When following basic security best practices, the license server must be accessible within a Local Area Network (LAN), such as a corporate network. This significantly limits exposure to the Boost related vulnerability.
- Firewalls and other policies, which are used by the enterprise to protect their own resources, must be extended to machines running FlexNet Publisher license server.

CryptoPP

Reverera has received reports from customers, indicating a couple of CVEs (Common Vulnerabilities and Exposures) in the CryptoPP version 8.9. If you are not using Trusted Storage-based licensing, the CryptoPP related vulnerabilities can be safely ignored.

Vulnerabilities

The following vulnerabilities are detected in the CryptoPP software:

- **Vulnerability ID: CVE-2024-28285**—The CVE-2024-28285 vulnerability exists in the CryptoPP's ElGamal encryption algorithm. This vulnerability is rated as critical severity. FlexNet Publisher is not vulnerable, as it does not use ElGamal encryption in any component. Therefore, FlexNet Publisher is not affected.
- **Vulnerability ID: CVE-2023-50979**—The CVE-2023-50979 vulnerability exists in the RSA Timing Side-Channel. This vulnerability is rated as medium severity. FlexNet Publisher is not vulnerable, as it does not use RSA PKCS#1 v1.5 padding in any component. Therefore, FlexNet Publisher is not affected.
- **Vulnerability ID: CVE-2023-50980 and CVE-2023-50981**—These vulnerabilities relate to malformed key processing and can potentially cause a denial-of-service when specially crafted, untrusted cryptographic keys are processed. These vulnerabilities are rated as high severity. FlexNet Publisher is not vulnerable, as it uses only pre-generated and trusted cryptographic vendor keys that are created by Revenera. FlexNet Publisher's architecture does not expose any API that would allow such arbitrary keys to be imported and there is no mechanism for introducing such malicious data into the system. Therefore, FlexNet Publisher is not affected.

Legal Information

Copyright Notice

Copyright © 2026 Flexera Software

This publication contains proprietary and confidential information and creative works owned by Flexera Software and its licensors, if any. Any use, copying, publication, distribution, display, modification, or transmission of such publication in whole or in part in any form or by any means without the prior express written permission of Flexera Software is strictly prohibited. Except where expressly provided by Flexera Software in writing, possession of this publication shall not be construed to confer any license or rights under any Flexera Software intellectual property rights, whether by estoppel, implication, or otherwise.

All copies of the technology and related information, if allowed by Flexera Software, must display this notice of copyright and ownership in full.

Intellectual Property

For a list of trademarks and patents that are owned by Flexera Software, see <https://www.revenera.com/legal/intellectual-property.html>. All other brand and product names mentioned in Flexera Software products, product documentation, and marketing materials are the trademarks and registered trademarks of their respective owners.

Restricted Rights Legend

The Software is commercial computer software. If the user or licensee of the Software is an agency, department, or other entity of the United States Government, the use, duplication, reproduction, release, modification, disclosure, or transfer of the Software, or any related documentation of any kind, including technical data and manuals, is restricted by a license agreement or by the terms of this Agreement in accordance with Federal Acquisition Regulation 12.212 for civilian purposes and Defense Federal Acquisition Regulation Supplement 227.7202 for military purposes. The Software was developed fully at private expense. All other use is prohibited.