

# Common Criteria Maintenance Report

---

## Cisco cEdge Routers running IOS XE 17.12.04 with SD-WAN 20.12.06.1



CAN-654-LSS

1 April 2026

v1.0



Communications Security  
Establishment Canada  
Canadian Centre  
for Cyber Security

Centre de la sécurité des  
télécommunications Canada  
Centre canadien  
pour la cybersécurité

Canada

## Foreword

---

This maintenance report is an UNCLASSIFIED publication, issued under the authority of the Chief, Communications Security Establishment (CSE).

The Information Technology (IT) product identified in this report has been previously evaluated at an approved testing laboratory established under the Canadian Centre for Cyber Security (a branch of CSE). This report applies only to the identified version and release of the product in its evaluated configuration.

This report is not an endorsement of the IT product by Canadian Centre for Cyber Security, or any other organization that recognizes or gives effect to this report. Furthermore, no warranty for the IT product by the Canadian Centre for Cyber Security, or any other organization that recognizes or gives effect to this report is either expressed or implied.

If your organization has identified a requirement for this report based on business needs and would like more detailed information, please contact:

Canadian Centre for Cyber Security

Contact Centre and Information Services

[contact@cyber.gc.ca](mailto:contact@cyber.gc.ca) | 1-833-CYBER-88 (1-833-292-3788)



# TABLE OF CONTENTS

Foreword..... 1

Executive Summary CAN-654-LSS ..... 3

Description of Changes ..... 4

    Description of Changes in the Maintained Target of Evaluation ..... 4

    Affected Developer Evidence ..... 5

Conclusion..... 6

References ..... 7



## Executive Summary CAN-654-LSS

---

The purpose of this document is to summarize and present the Canadian Common Criteria program's findings regarding the assurance maintenance of **Cisco cEdge Routers running IOS XE 17.12.04 with SD-WAN 20.12.06.1**, hereafter referred to as the maintained Target of Evaluation, or maintained TOE.

An Impact Analysis Report was submitted to the Canadian Common Criteria Program to extend the validity of the Common Criteria certificate previously awarded to **Cisco cEdge Routers running IOS XE 17.12.04 with SD-WAN 20.12.04** from **Cisco Systems, Inc .**

The process to achieve this is described in Assurance Continuity: CCRA Requirements, version 3.0, March 2023. In accordance with the requirements of this process, the Impact Analysis Report describes all changes made to the product and/or its IT environment, all resulting changes made to the evaluation evidence, and the security impact of the changes.

The Canadian Centre for Cyber Security, as the Certification Body, declares that the assurance gained during the original certification has been preserved.



## Description of Changes

The following characterizes the changes implemented in the maintained TOE and/or the environment. For each change, it was verified that there were no required changes to the security functional requirements in the Security Target.

<b>Original TOE</b>	Cisco cEdge Routers running IOS XE 17.12.04 with SD-WAN 20.12.04
<b>Maintained TOE</b>	Cisco cEdge Routers running IOS XE 17.12.04 with SD-WAN 20.12.06.1
<b>Developer</b>	Cisco Systems, Inc

## Description of Changes in the Maintained Target of Evaluation

The changes in the maintained TOE comprise the following:

- The TOE was patched (SD-WAN 20.12.06.1) to address the following CVEs:

<ul style="list-style-type: none"> <li>○ CVE-2026-20133</li> <li>○ CVE-2026-20126</li> <li>○ CVE-2026-20129</li> <li>○ CVE-2026-20128</li> <li>○ CVE-2026-20122</li> <li>○ CVE-2026-20127</li> <li>○ CVE-2026-20108</li> <li>○ CVE-2025-20339</li> </ul>	<ul style="list-style-type: none"> <li>○ CVE-2025-20221</li> <li>○ CVE-2025-20216</li> <li>○ CVE-2025-20213</li> <li>○ CVE-2025-20187</li> <li>○ CVE-2025-20157</li> <li>○ CVE-2025-20155</li> <li>○ CVE-2025-20147</li> <li>○ CVE-2025-20122</li> </ul>
--	--

- Minor bug fixes and stability updates that do not impact evaluated functionality of the TOE and maintain the security requirements as specified in the certified Security Target



## Affected Developer Evidence

---

Modifications to the product necessitated changes to the following developer evidence that was previously submitted in support of the original evaluation:

- The following documents were updated to reflect the new SD-WAN controller software version (20.12.6.1):
  - Security Target Cisco cEdge Routers running IOS XE 17.12 with SD-WAN 20.12, 2026-04-01, v1.4
  - Cisco cEdge Routers running IOS XE 17.12 with SD-WAN 20.12 Common Criteria Operational User Guidance and Preparative Procedures, 2026-04-01, v1.0



## Conclusion

---

As all changes to the maintained TOE were classified as minor, the Certification Body has determined that assurance maintenance is appropriate and that re-evaluation is not required. The assurance maintenance for the TOE was conducted in accordance with the provisions of the Canadian Common Criteria Program, and the conclusion reached is consistent with the evidence presented.

Functional and regression testing of the maintained TOE confirmed that the assurance gained during the original certification has been preserved.



## References

Reference
Assurance Continuity: CCRA Requirements, V3.0, March 2023
Certification Report Cisco cEdge Routers running IOS XE 17.12 with SD-WAN 20.12, 2024-12-18, v1.0
Security Target Cisco cEdge Routers running IOS XE 17.12 with SD-WAN 20.12, 2026-04-01, v1.4
Post Certification Patching Report Cisco cEdge Routers running IOS XE 17.12 with SD-WAN 20.12, 2026-04-01, v0.1

