Communications Security Establishment
Centre de la sécurité des télécommunications

CANADIAN CENTRE FOR CYBER SECURITY

COMMON CRITERIA MAINTENANCE REPORT

NetScaler Version 13.1 Build 37.241

5 September 2025

607-LSS

V1.0

FOREWORD

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

The IT product identified in this report has been previously evaluated at an approved Common Criteria testing lab established under the Canadian Common Criteria program using the Common Methodology for IT Security Evaluation, Version 3.1 Revision 5, for conformance to the Common Criteria for IT Security Evaluation, Version 3.1 Revision 5.

This report is not an endorsement of the IT product by the Canadian Centre for Cyber Security, and no warranty of the IT product by the Canadian Centre for Cyber Security is expressed or implied.

If your organization has identified a requirement for this maintenance 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 | 1-833-CYBER-88 (1-833-292-3788)

TABLE OF CONTENTS

1 INTRODUCTION

An Impact Analysis Report was submitted to the Canadian Common Criteria program to extend the validity of the Common Criteria certificate previously awarded to **NetScaler Version 13.1 Build 37.201** from **Cloud Software Group.**

The process to achieve this under mutual recognition 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 purpose of this document is to summarize and present the Canadian Common Criteria program's findings regarding the assurance maintenance of **NetScaler Version 13.1 Build 37.241** , hereafter referred to as the maintained Target of Evaluation or maintained TOE.

2 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.

Table 1: TOE Identification

Original TOE	**NetScaler Version 13.1 Build 37.201**
Maintained TOE	**NetScaler Version 13.1 Build 37.241**
Developer	**Cloud Software Group.**

2.1 DESCRIPTION OF CHANGES IN THE MAINTAINED TARGET OF EVALUATION

The changes in the maintained TOE comprise the following:

- The TOE software version has changed from NetScaler Version 13.1 Build 37.201 to NetScaler Version 13.1 Build 37.241 to address the following CVEs:
  - CVE-2025-7775: Memory overflow vulnerability leading to Remote Code Execution and/or Denial of Service.
  - CVE-2025-7776: Memory overflow vulnerability leading to unpredictable or erroneous behavior and Denial of Service
  - CVE-2025-8424: Improper access control on the NetScaler Management Interface
  - CVE-2025-6543: Memory overflow vulnerability leading to unintended control flow and Denial of Service
  - CVE-2025-5349: Improper access control on the NetScaler Management Interface
  - CVE-2025-5777: Insufficient input validation leading to memory overread
  - CVE-2024-8534: Memory safety vulnerability leading to memory corruption and Denial of Service.
  - CVE-2024-8535: Authenticated user can access unintended user capabilities
- Bug fixes and feature enhancements were also made to functionality that was not included in the scope of the original evaluation.

2.2 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 Security Target was updated as follows:
  - New date and version
  - Updated TOE reference to reflect new build number (37.241)

3 CONCLUSIONS

Through functional and regression testing of the maintained TOE, assurance gained in the original TOE certification was maintained. As all the changes to the maintained TOE have been classified as minor, it is the conclusion of the CB that the maintained TOE is appropriate for assurance maintenance and re-evaluation is not required.

The assurance maintenance of the TOE has been conducted in accordance with the provisions of the Canadian Common Criteria Scheme and the conclusions are consistent with the evidence adduced. This is not an endorsement of the IT product by the Cyber Centre or by any other organization that recognizes or gives effect to this certificate, and no warranty of the IT product by the Cyber Centre or by any other organization that recognizes or gives effect to this certificate, is expressed or implied.

4 REFERENCES

Reference
Assurance Continuity: CCRA Requirements, V3.0, March 2023.
Certification Report NetScaler Version 13.1 Build 37.201, 2024-12-02, v1.0.
Security Target NetScaler Version 13.1 Build 37.241, 2025-09-03, v2.5.
Impact Analysis Report, NetScaler 13.1 NDcPP Build 37.201 to 37.241, 2025-09-05, Version 1.0.