Communications Security Establishment | Centre de la sécurité des télécommunications

CANADIAN CENTRE FOR CYBER SECURITY

COMMON CRITERIA MAINTENANCE REPORT

Fortinet FortiGate w/ FortiOS v5.6.7 Build 6022

26 August 2019

383-7-159

V1.0

© Government of Canada
This document is the property of the Government of Canada. It shall not be altered, distributed beyond its intended audience, produced, reproduced or published, in whole or in any substantial part thereof, without the express permission of CSE.

Canada

FOREWORD

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

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

Contact Centre and Information Services
Edward Drake Building
contact@cyber.gc.ca | 1-833-CYBER-88 (1-833-292-3788)

OVERVIEW

This is a Maintenance Report for Fortinet FortiGate w/ FortiOS v5.6.7 Build 6022 (hereafter referred to the TOE), that satisfies the requirements outlined in Assurance Continuity: CCRA Requirements, v2.1, June 2012. In accordance with those requirements, an Impact Assessment Report was submitted which describes the changes implemented in the TOE, (the maintained Target of Evaluation), the evidence updated as a result of the changes and the security impact of the changes.

TABLE OF CONTENTS

1 CHANGES

The following characterizes the changes implemented in the TOE and/or the environment. For each change, it was verified that there were no required changes to the security functional requirements in the ST, and thorough functional and regression testing was conducted by the developer to ensure that the assurance in the Target of Evaluation (TOE) was maintained.

1.1 DESCRIPTION OF CHANGES IN THE MAINTAINED TARGET OF EVALUATION

The changes in the TOE comprise fixes for the following bugs/vulnerabilities:

- ZebOS; unprivileged, authenticated user can change the routing settings (CVE-2018-13371)
- FortiOS SSL VPN web portal Host Header Redirection (CVE-2018-13384)
- Unauthenticated SSL VPN users password modification (CVE-2018-13382)
- SSL VPN web mode internal server issue
- FortiOS reflected XSS in the SSL VPN web portal error page parameters (CVE-2019-5586)
- FortiOS; buffer overflow via Javascript HREF Content (CVE-2018-13383)
- FortiOS; directory traversal via SSL VPN (CVE-2018-13379)
- Cross Site Scripting via SSL VPN Portal (CVE-2018-13380)
- FortiOS SSL VPN buffer overrun through POST message payload (CVE-2018-13381)

1.2 AFFECTED DEVELOPER EVIDENCE

Modifications to the product necessitated changes to a subset of the developer evidence that was previously submitted for the TOE. The set of affected developer evidence was identified in the IAR.

Modifications to the security target were made to reflect the new product versions.

2 CONCLUSIONS

Through functional and regression testing of the TOE, assurance gained in the original TOE certification was maintained. As all of 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 continuity and re-evaluation is not required.

The IT product identified in this report has been previously evaluated at an approved evaluation facility established under the Canadian Common Criteria Evaluation and Certification Scheme using the Common Methodology for IT Security Evaluation, Version 3.1 Revision 4, for conformance to the Common Criteria for IT Security Evaluation, Version 3.1 Revision 4.

This is not an endorsement of the IT product by CSE or by any other organization that recognizes or gives effect to this certificate, and no warranty of the IT product by CSE or by any other organization that recognizes or gives effect to this certificate, is expressed or implied.

2.1 REFERENCES

Reference
Assurance Continuity: CCRA Requirements, v2.1, June 2012
Certification Report for Fortinet FortiGate v5.6.7, v1.0, 22/05/2019
Security Target for Fortinet FortiGate v5.6.7, v1.4, 09/08/2019