Agenzia per la Cybersicurezza Nazionale

Servizio Certificazione e Vigilanza

Organismo di Certificazione della Sicurezza Informatica

Re-Assessment Report

Ivanti Security Controls 2022.2 (Version 9.5.9293.0)

Certificate 11/23

OCSI/AVA/CCL/01/2025/RV

Version 1.0

11 August 2025

Courtesy translation

Disclaimer: This English language translation is provided for informational purposes only. It is not intended to substitute the official document and has no legal value. The original Italian language version of the document is the only approved and official version.

1 Document revisions

Version	Author	Information	Date
1.0	OCSI	First issue	11/08/2025

2 Table of contents

3 Acronyms

3.1 National scheme

DPCM	Decreto del Presidente del Consiglio dei Ministri
LGP	Linea Guida Provvisoria
LVS	Laboratorio per la Valutazione della Sicurezza
NIS	Nota Informativa dello Schema
OCSI	Organismo di Certificazione della Sicurezza Informatica

3.2 CC and CEM

CC	Common Criteria
CCRA	Common Criteria Recognition Arrangement
CEM	Common Evaluation Methodology
cPP	collaborative Protection Profile
EAL	Evaluation Assurance Level
ETR	Evaluation Technical Report
PP	Protection Profile
SOGIS-MRA	Senior Officials Group Information Systems Security Mutual Recognition Arrangement
ST	Security Target
TOE	Target of Evaluation

3.3 Other acronyms

CVE	Common Vulnerability and Exposure

4 References

4.1 Normative references and national scheme documents

[CC1] CCMB-2017-04-001, “Common Criteria for Information Technology Security Evaluation, Part 1 – Introduction and general model”, Version 3.1, Revision 5, April 2017

[CC2] CCMB-2017-04-002, “Common Criteria for Information Technology Security Evaluation, Part 2 – Security functional components”, Version 3.1, Revision 5, April 2017

[CC3] CCMB-2017-04-003, “Common Criteria for Information Technology Security Evaluation, Part 3 – Security assurance components”, Version 3.1, Revision 5, April 2017

[CCRA] “Arrangement on the Recognition of Common Criteria Certificates In the field of Information Technology Security”, July 2014

[CEM] CCMB-2017-04-004, “Common Methodology for Information Technology Security Evaluation – Evaluation methodology”, Version 3.1, Revision 5, April 2017

[LGP1] Schema nazionale per la valutazione e certificazione della sicurezza di sistemi e prodotti nel settore della tecnologia dell’informazione - Descrizione Generale dello Schema Nazionale - Linee Guida Provvisorie - parte 1 – LGP1 versione 1.0, dicembre 2004

[LGP2] Schema nazionale per la valutazione e certificazione della sicurezza di sistemi e prodotti nel settore della tecnologia dell’informazione - Accreditamento degli LVS e abilitazione degli Assistenti - Linee Guida Provvisorie - parte 2 – LGP2 versione 1.0, dicembre 2004

[LGP3] Schema nazionale per la valutazione e certificazione della sicurezza di sistemi e prodotti nel settore della tecnologia dell’informazione - Procedure di valutazione - Linee Guida Provvisorie - parte 3 – LGP3, versione 1.0, dicembre 2004

[NIS1] Organismo di certificazione della sicurezza informatica, Nota Informativa dello Schema N. 1/23 – Modifiche alla LGP1, versione 1.1, agosto 2023

[NIS2] Organismo di certificazione della sicurezza informatica, Nota Informativa dello Schema N. 2/23 – Modifiche alla LGP2, versione 1.1, agosto 2023

[NIS3] Organismo di certificazione della sicurezza informatica, Nota Informativa dello Schema N. 3/23 – Modifiche alla LGP3, versione 1.1, agosto 2023

[NIS4] Organismo di certificazione della sicurezza informatica, Nota Informativa dello Schema N. 4/23 – Gestione nel tempo delle garanzie di prodotti certificati, versione 1.1, agosto 2023

[SOGIS] “Mutual Recognition Agreement of Information Technology Security Evaluation Certificates”, Version 3, January 2010

4.2 Technical documents

[AC] Assurance Continuity – CCRA requirements, v.3.1, 29 February 2024

[AGD] Ivanti Security Controls 2022.2 Guidance Documentation Supplement, version: 0.10, 11 August 2023

[RC] Certification Report Ivanti Security Controls 2022.2 (Version 9.5.9293.0) OCSI/CERT/CCL/06/2022/RC Version 1.0 14 November 2023

[ETRv3] Evaluation Technical Report Re-Assessment of Ivanti Security Controls 2022.2 (Version 9.5.9293.0) based on CC Assurance Level EAL2 augmented ALC_FLR.2 based on ISO/IEC 18045:2008 Information technology - Security techniques - Methodology for IT security evaluation, IVANTIREA-009_ETR_v3, 2025-06-11, version v3

[ST] Ivanti Security Controls 2022.2 Security Target, Evaluation Assurance Level (EAL): EAL 2+, Document Version: 0.11, November 7, 2023

5 Mutual recognition in SOGIS-MRA and CCRA

The re-assessment activity of certified products is performed in accordance with the provisions of [NIS4] and [AC] that is adopted within both SOGIS-MRA and CCRA mutual recognition.

6 Statement of certification

The Target of Evaluation (TOE) is the product Ivanti Security Controls 2022.2 (Version 9.5.9293.0), developed by Ivanti.

The TOE is an integrated software solution providing patch management, asset inventory, IT administration, and reporting functionality. These functions are supported through the Security Controls application.

The TOE is a Windows-based software solution that is comprised of the following components:

- Security Controls Console.
- Security Controls Agent.
- Security Controls Deployment Tool Chain.

The re-assessment has been conducted in accordance with the requirements established by the Italian Scheme for the evaluation and certification of security systems and products in the field of information technology and expressed in the Scheme Information Note [NIS4]. The Scheme is operated by the Italian Certification Body “Organismo di Certificazione della Sicurezza Informatica (OCSI)”, established by the Prime Minister Decree (DPCM) of 30 October 2003 (O.J. n.98 of 27 April 2004).

The objective of the re-assessment for a certified product is to confirm, at the date of issuance of this report, that it still complies with the security assurance requirements specified in the associated Security Target [ST]. The evaluation activities have been carried out in accordance with the Common Criteria Part 3 [CC3] and the Common Evaluation Methodology [CEM].

7 Summary of evaluation activities

7.1 Introduction

This document reports the outcome of the re-assesment activity for the product “Ivanti Security Controls 2022.2 (Version 9.5.9293.0)” performed in accordance with the assurance requirements of Common Criteria class AVA.

This Re-assessment Report should be consulted in conjunction with the Security Target [ST], specifying the functional and assurance requirements and the intended operational environment.

7.2 Executive Summary

TOE name	Ivanti Security Controls 2022.2 (Version 9.5.9293.0)
Security Target	Ivanti Security Controls 2022.2 Security Target, version: 0.11, 7 November 2023 [ST]
Certification Report	Certification Report Ivanti Security Controls 2022.2 (Version 9.5.9293.0) OCSI/CERT/CCL/06/2022/RC Version 1.0 14 November 2023 [RC]
Developer	Ivanti, Inc.
Sponsor	Corsec Security, Inc.
LVS	CCLab – The Agile Cybersecurity Laboratory (Budapest site)

The re-assessment results apply only to the version of the product shown in the Certification Report [RC] and only if the operational environment assumptions described in the Security Target [ST] are fulfilled.

7.3 Evaluation conduct

The evaluation has been conducted in accordance with the requirements established by the Italian Scheme for the evaluation and certification of security systems and products in the field of information technology and expressed in the Scheme Information Note [NIS4].

The purpose of the evaluation is to provide an update, at the issuance date of the present Re-Assessment Report, of the vulnerability analysis of the certified product to confirm the security assurance requirements of the certified TOE to meet the requirements stated in the relevant Security Target [ST]

The Certification Body OCSI has supervised the conduct of the evaluation performed by the evaluation facility (LVS) CCLab – The Agile Cybersecurity Laboratory (Budapest site).

The evaluation activity was completed on 11 June 2025 with the issuance by the LVS of the Evaluation Technical Report [ETRv3], which was approved by the Certification Body on 2 July 2025. Then, the Certification Body issued this Re-Assessment Report.

8 Evaluation outcome

8.1 Evaluation results

Following the analysis of the Evaluation Technical Report [ETRv3] issued by the LVS CCLab – The Agile Cybersecurity Laboratory (Budapest site) and accompanying evaluation evidence, the Certification Body concluded that the TOE "Ivanti Security Controls 2022.2 (Version 9.5.9293.0)" still meets the security assurance requirements of Part 3 of the Common Criteria [CC3] claimed in [RC].

Table 1 summarizes the final verdict of each activity carried out by the LVS.

Assurance classes and components		**Verdict**
Vulnerability assessment	**Class AVA**	Pass
Vulnerability analysis	AVA_VAN.2	Pass

Table 1 - - Final verdicts for assurance requirements

8.2 Recommendations

The conclusions of the Certification Body (OCSI) are summarized in section 6 (Statement of Certification).

Potential users of the product "Ivanti Security Controls 2022.2 (Version 9.5.9293.0)" are recommended to review and understand the specific purpose of certification by reading this Re-assessment Report and the Certification Report [CR] together with the Security Target [ST].

The TOE must be used according to the Security Objectives for the operational environment specified in section 4.2 of the Security Target [ST]. It is assumed that, in the operational environment of the TOE, all the Organizational Security Policies and the Assumptions described, respectively, in section 3.2 and 3.3 of the Security Target [ST] are respected.

9 Annex A – Test activity

9.1 Vulnerability analysis and penetration tests

This re-assessment was conducted to evaluate the impact of the following public vulnerabilities on certificate 11/23 issued by OCSI within certification process OCSI/CERT/CCL/06/2022 ([RC]).

Further information are provided on these CVEs in the vendor website[1].

CVE	Description
CVE-2024-10251	Under specific circumstances, insecure permissions in Ivanti Security Controls before version 2024.4.1 allows a local authenticated attacker to achieve local privilege escalation.
CVE-2024-10256	Insufficient permissions in Ivanti Patch SDK before version 9.7.703 allows a local authenticated attacker to delete arbitrary files.

Table 2 – CVEs applicable to the TOE

The Evaluator conducted an overall update of the vulnerability analysis including the abovementioned CVEs with the following approach.

For the execution of the vulnerability analysis, a test environment was set up at the LVS site. The Evaluator verified the system configuration according to the documentation already provided by the developer [AGD] and the Security Target [ST].

The Evaluator performed a search of public information sources, investigated the potential vulnerabilities analysed and described in [CR] and included the abovementioned CVEs. A total of 11 potential vulnerabilities were considered for further in-depth investigation by the Evaluator.

At the end of the evaluation, the Evaluator determined that only CVE-2024-10251 and CVE-2024-10256 could be considered actually applicable to the TOE in the certified configuration but could be exploited only by an attacker with attack potential beyond Basic.

Therefore, it is possible to conclude that the two applicable vulnerabilities can be considered as residual vulnerabilities, and they do not impact the assurance baseline of the certificate which can be then regarded still valid.

[1] Information on CVE-2024-10251 (https://forums.ivanti.com/s/article/Security-Advisory-Ivanti-Security-Controls-iSec-CVE-2024-10251?language=en_US)
Information on CVE-2024-10256 (https://forums.ivanti.com/s/article/Security-Advisory-Ivanti-Patch-SDK-CVE-2024-10256?language=en_US)