ADISA
ASSET DISPOSAL & INFORMATION
SECURITY ALLIANCE

Product Claims Test
Application Number ADPC0056
AllWipe Oy Ltd

Author: Professor Andrew Blyth

Revision 1.0
Date: January 7, 2019
Distribution: Confidential

DISCLAIMER

The Product Claims Test is presented as the outcome of a specific test ran in laboratory environment under controlled conditions. Use of this certified product for the purpose of sanitizing data from devices tested needs to be done so after a risk assessment process. ADISA reserves the right to review the validity of this award upon changes in threat landscape.

LIABILITY

ADISA accepts no liability for any claims resulting from the use of the product tested.

REVISION HISTORY

07.01.2019	Revision 1.0 issued to Ariel Figueras

Asset Disposal and Information Security Alliance Limited

Phone: 0044 845 557 7726

Web: www.adisa.global

Registration Number: 07390092
Registered Office: 31 Thrales End Business Centre, Thrales End Lane, Harpenden, AL5 3EJ, United Kingdom

Contents

1.0 Executive Summary

This is the final report detailing the findings in relation to the execution of the ADISA Testing Methodology on Claims Test ADPC0056 submitted by AllWipe Oy Ltd for product YouWipe Data Erasure. The claims test was carried out in accordance with ADISA Claims Testing (ACT) v1.0 and supporting document ADISA Testing Methodology v1.0, both of which are available from ADISA.

The claim made for the test was:

> *"The company, AllWipe Oy Ltd., and the software, Youwipe data erasure, version 3.0, when used in accordance with user manual (3.3.18), will overwrite using algorithm "Ext. HMG Infosec High", all user data on the sample media to ensure that data cannot be recovered using forensic techniques aligned to ADISA Test Level 2." – Claim Number ADPC0056.*

One Solid State Device was submitted as part of this test and this is listed below:

Family	***Model***	***Test Level***
Western Digital 250Gb NVME SSD	WDS250G2X0C	2

Table 1 – Devices Tested

After testing it is confirmed that the AllWipe Oy **claim is true** for the device tested up to Test Level 1 and 2 results. Those devices are:

- Western Digital 250Gb NVME SSD Model WDS250G2X0C

2.0 Test Level 1 Testing on Solid State Media

2.1 Methodology.

This test phase is designed to evaluate the claim made by recreating an attack by a threat adversary utilising standard COTS forensic tools and techniques. (e.g. Encase V7.12.01 and Forensic Explorer V4). For each device the following methodology is performed.

1. The Software was configured in accordance with the manufacturer's instructions.
2. If present the DCO and HPA are removed from the test devices
3. Structure data of a known type is written to ever positive logical block address (LBA)
4. To create a Base Image for comparison the device is then forensically images.
5. The device was then erased using the software in accordance with the manufacturer's instructions.
6. The device was then imaged to create the test image.
7. The test image was then data carved to identify any images and the results compares and contrasted with the base-image constructed in step 5.

2.2 Test Results.

Test Level 1 Summary Results

Test Level 1 replicated an attack on this device being made by an aggressor with capabilities outlined below.

Risk Level	Threat Actor and Compromise Methods	Test Level
1 (Very Low)	Casual or opportunistic threat actor only able to mount high-level non-invasive and non-destructive software attacks utilising freeware, OS tools and COTS products.	1
2 (Low)	Commercial data recovery organisation able to mount non-invasive and non-destructive software attacks and hardware attacks.	1

The Results of Test Level 1

Family	***Model***	**Result**
Western Digital 250Gb NVME SSD	WDS250G2X0C	**PASS**

- Pass means that YouWipe data erasure, version 3.0 mitigates the threat posed by the Threat Actors holding the capabilities outlined by Test Level 1.

3.0 Test Level 2 Testing Solid State Drives

3.1 Methodology.

This test phase is designed to evaluate the claim made by recreating an attack by a threat adversary utilising standard intrusive/destructive testing tools designed to read data directly off the device at the platter/chip level.

For each computer hard drive device, the following methodology is performed:

1. The device is connected to a target PC and place in a stable state.
2. Structured data, the string "ISRG", was written to every logical block address on the hard drive.
3. The device was then imaged using Access Data/FTK to create a base-line forensic image.
4. The device was then erased using the test applicant's software in accordance with the manufacturer's instructions.
5. The device was then analysed use the following tools and techniques to create a series of forensic images that are compared and contrasted with the base-line forensic image to ensure that all structured data has been removed. For this test, there is no tolerance for remnant structured data and the result is a straight Pass or Fail.
   a. Software based forensic tools/techniques such as:
      i. Standard commercial tools and techniques such as Access Data/FTK and ENCase;
      ii. State of the art data recovery tools such as PC3000 SSD;
      iii. Customer designed data recovery software.
   b. Hardware/Chip based forensic tools/techniques such as:
      i. Flash/NAND TSOP/BGA chip readers;
      ii. State of the art data recovery tools such as PC3000 FLASH and Rusolut;
      iii. Customer designed data recovery software/hardware.

3.2 Test Results.

Test Level 2 Summary Results

Test Level 2 replicated an attack on this device being made by an aggressor with capabilities outlined below.

Risk Level	Threat Actor and Compromise Methods	Test Level
3 (Medium)	Commercial computer forensics organisation able to mount both non-invasive/non-destructive and invasive/non-destructive software and hardware attack, utilising COTS products.	2
4 (High)	Commercial data recovery and computer forensics organisation able to mount both non-invasive/non-destructive and invasive/ non-destructive software and hardware attack, utilising both COTS and bespoke utilities.	2

The Results of Test Level 2.

Family	*Model*	Result
Western Digital 250Gb NVME SSD	WDS250G2X0C	**PASS**

- Pass means that YouWipe data erasure, version 3.0 mitigates the threat posed by the Threat Actors holding the capabilities outlined by Test Level 2.

4.0 Summary and Conclusions

The Western Digital 250Gb NVME SSD media tested passed the claims test as all-forensic data recovery techniques up to and including ADISA Test Level 2 failed to recover any data. The product evaluated was YouWipe data erasure, version 3.0.

Claims Test Carried Out By: Professor Andrew Blyth, PhD.

Signature:

Date: 07.01.2019