Microsoft Corporation
SP 800-90B Public Use Document
(Non-Proprietary)

Windows OS Loader Entropy Source

Microsoft Windows Server 2022
(Standard and Datacenter Editions)

Prepared By	Microsoft Corporation One Microsoft Way Redmond, WA 98052-6399
Version Number	1.0
Updated On	August 23, 2024

COPYRIGHT AND DISCLAIMER

The information contained in this document represents the current view of Microsoft Corporation on the issues discussed as of the date of publication. Because Microsoft must respond to changing market conditions, it should not be interpreted to be a commitment on the part of Microsoft, and Microsoft cannot guarantee the accuracy of any information presented after the date of publication.

This document is for informational purposes only. MICROSOFT MAKES NO WARRANTIES, EXPRESS OR IMPLIED, AS TO THE INFORMATION IN THIS DOCUMENT.

Complying with all applicable copyright laws is the responsibility of the user. This work is licensed under the Creative Commons Attribution-NoDerivs-NonCommercial VLicense (which allows redistribution of the work). To view a copy of this license, visithttp://creativecommons.org/licenses/by-nd-nc/1.0/ or send a letter to Creative Commons, 559 Nathan Abbott Way, Stanford, California 94305, USA.

Microsoft may have patents, patent applications, trademarks, copyrights, or other intellectual property rights covering subject matter in this document. Except as expressly provided in any written license agreement from Microsoft, the furnishing of this document does not give you any license to these patents, trademarks, copyrights, or other intellectual property.

The example companies, organizations, products, people and events depicted herein are fictitious. No association with any real company, organization, product, person or event is intended or should be inferred.

© 2024 Microsoft Corporation. All rights reserved.

Microsoft, Active Directory, Visual Basic, Visual Studio, Windows, the Windows logo, Windows NT, and Windows Server are either registered trademarks or trademarks of Microsoft Corporation in the United States and/or other countries.

The names of actual companies and products mentioned herein may be the trademarks of their respective owners.

This Public Use Document is non-proprietary and may be reproduced only in its original entirety without revision.

Contents

Table of Figures iii

Table of Tables iv

Version History iv

1 Description 1

2 Security Boundary 1

3 Operating Conditions 2

4 Configuration Settings 3

5 Physical Security Mechanisms 3

6 Conceptual Interfaces 3

6.1 GetEntropy 3

6.2 GetNoise 3

6.3 Health Test 3

7 Min-Entropy Rate 3

8 Health Tests 4

9 Maintenance 4

10 Required Testing 4

Table of Figures

Figure 1: Windows OS Loader Entropy Source Boundary 2

© 2024 Microsoft. All Rights Reserved

This Public Use Document is non-proprietary and may be reproduced only in its original entirety without revision.

Table of Tables

Table 1: Version History iv
Table 2: Tested Platforms 1
Table 3: Test Platform Operating Conditions 2

Version History

Version	Date	Description
1.0	March 25, 2024	Draft submitted to CMVP for entropy validation.

Table 1: Version History

© 2024 Microsoft. All Rights Reserved

This Public Use Document is non-proprietary and may be reproduced only in its original entirety without revision.

1 Description

The Windows OS Loader entropy source consists of a Physical (P) noise source and conditioning chain contained in an Intel processor, supplemented with a vetted conditioning component implemented in software by Microsoft. The Intel portion of the entropy source is accessed via the RDSEED machine instruction, the software portion is implemented within the Windows OS Loader executable binary (winload.efi).

This noise source follows the non-IID track and makes no IID claims.

This document is based on the Windows OS Loader Entropy Assessment Report for Windows Server 2022 and was tested on the following platforms:

Operating System(s)	Processor
Microsoft Windows Server 2022	Intel® Xeon® Gold and Intel® Xeon® Platinum Processor 28 Die with FCLGA3647 Package

Table 2: Tested Platforms

The "Intel® Xeon® Gold and Intel® Xeon® Platinum Processor 28 Die with FCLGA3647 Package" processor is also known as "Intel Xeon Gold" in this report.

2 Security Boundary

The security boundary of the Windows OS Loader Entropy Source is shown in Figure 1 below. Note that the supplemental data is not included in the NIST SP 800-90B calculations with any entropy input in the design of this entropy source. The contents of the RDSEED Instruction box represent the noise source and the conditioning chain components as implemented by Intel in their processors.

© 2024 Microsoft. All Rights Reserved

This Public Use Document is non-proprietary and may be reproduced only in its original entirety without revision.

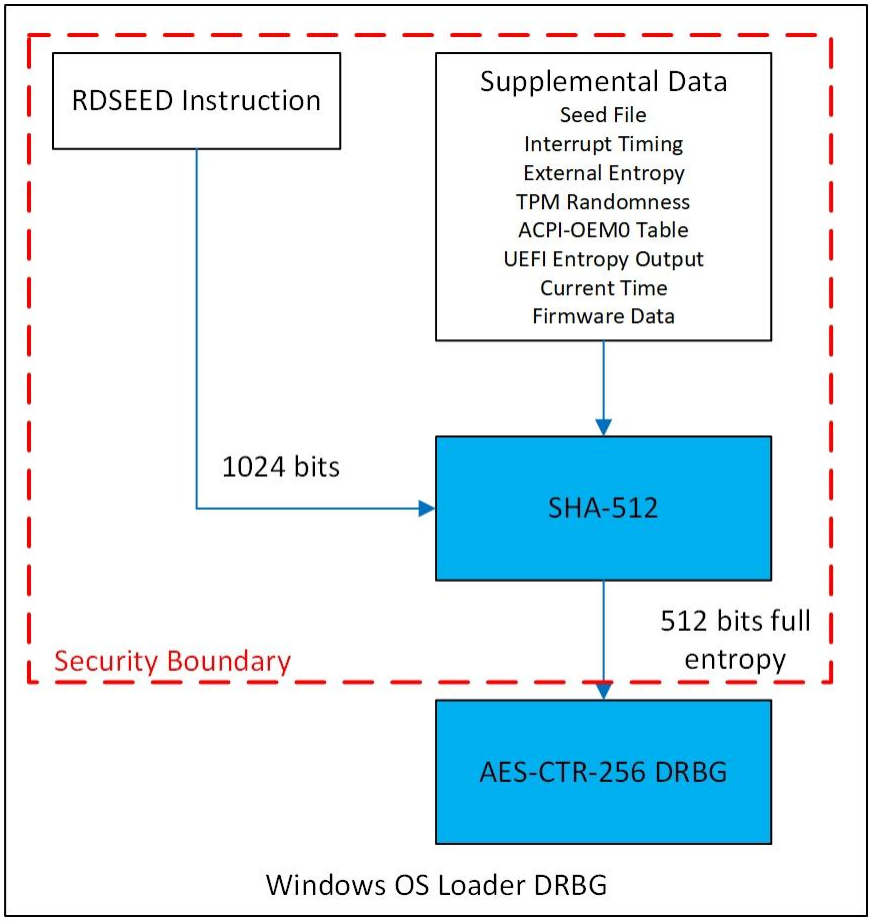


Figure 1: Windows OS Loader Entropy Source Boundary

3 Operating Conditions

Table 3 below summarizes the operating conditions under which the Windows OS Loader Entropy Source is expected to provide full entropy for each of the tested platforms.

Operating System	Processor	Temperature	Voltage
Microsoft Windows Server 2022	Intel Xeon Gold	0-91°C	Fixed via an internally regulated voltage supply to the noise source

Table 3: Test Platform Operating Conditions

© 2024 Microsoft. All Rights Reserved

This Public Use Document is non-proprietary and may be reproduced only in its original entirety without revision.

4 Configuration Settings

The Windows OS Loader entropy source does not expose any configuration settings to the user. All parameterization and settings are handled by the system at startup.

5 Physical Security Mechanisms

The Windows OS Loader entropy source does not provide any physical security mechanisms beyond that which is standard with the computer and processor in the tested platform.

6 Conceptual Interfaces

6.1 GetEntropy

The Windows OS Loader entropy source is used to initialize the Windows OS Loader deterministic random number generator; the conditioned entropy is not made accessible to users through an interface.

6.2 GetNoise

The Windows OS Loader entropy source does not provide an interface to obtain raw noise. However, the tools described in Section 10 of this document can be used by users to retrieve raw noise from the Intel RDSEED source.

6.3 Health Test

The Windows OS Loader entropy source does not provide an interface to trigger an on-demand health test. Because the Windows OS Loader Entropy Source is used as part of booting the Windows OS, a reboot executes all health tests again.

7 Min-Entropy Rate

The conditioning chain for the Windows OS Loader Entropy Source is as follows:

© 2024 Microsoft. All Rights Reserved

This Public Use Document is non-proprietary and may be reproduced only in its original entirety without revision.

1) Raw noise is collected from the Intel physical noise source
   - Health tests are performed
   - The H_submitter for this source is considered to be 0.6 bits per bit in a 512 bit output sample
2) This output is conditioned via an Intel implemented conditioning chain
3) 1024 bits are retrieved from RDSEED and passed to a Microsoft implemented SHA-512 vetted conditioning component

The output of the SHA-512 vetted conditioning component is the output of this entropy source. SP800-90B section 3.1.5.1.2 allows vetted conditioning components to claim full entropy, therefore each 512-bit output sample contains 512 bits of entropy, or full entropy.

The output of the Windows OS Loader Entropy Source is provided to a CAVP certified AES-CTR-DRBG, which is used to seed the next component in the Windows OS boot process in conjunction with additional output from Intel RDSEED Instruction.

8 Health Tests

The health tests for the Windows OS Loader entropy source are part of the continuous health tests in the Intel processor. These health tests satisfy all requirements of SP800-90B Section 4.3.

9 Maintenance

The Windows OS Loader entropy source does not have any user-required maintenance requirements.

10 Required Testing

SP 800-90B required tests were performed on data collected from the platforms in **Table 2: Tested Platforms** during validation. No further testing is required and the users must rely on the health tests to obtain assurance that the entropy source is operating correctly. The user must rely on these health tests to obtain assurance that the device is operating correctly because the user cannot access the raw noise data.

© 2024 Microsoft. All Rights Reserved

This Public Use Document is non-proprietary and may be reproduced only in its original entirety without revision.