MICROSOFT (MS) INTERNET INFORMATION SERVICES (IIS) 8.5 SECURITY TECHNICAL IMPLEMENTATION GUIDE (STIG) OVERVIEW

25 October 2023

Developed by DISA for the DOD

Trademark Information

Names, products, and services referenced within this document may be the trade names, trademarks, or service marks of their respective owners. References to commercial vendors and their products or services are provided strictly as a convenience to our users, and do not constitute or imply endorsement by the Defense Information Systems Agency (DISA) of any nonfederal entity, event, product, service, or enterprise.

TABLE OF CONTENTS

Page

1. INTRODUCTION 1

1.1 Executive Summary 1
1.2 Authority 1
1.3 Vulnerability Severity Category Code Definitions 1
1.4 STIG Distribution 2
1.5 SRG Compliance Reporting 2
1.6 Document Revisions 2
1.7 Other Considerations 2
1.8 Product Approval Disclaimer 3

2. ASSESSMENT CONSIDERATIONS 4

2.1 Product Overview 4
2.2 Performing a Web Server Assessment 4

LIST OF TABLES

Page

Table 1-1: Vulnerability Severity Category Code Definitions 2

1. INTRODUCTION

1.1 Executive Summary

The IIS 8.5 Server Security Technical Implementation Guide (STIG) provides direction on performing an assessment of a server being used in a web server role using IIS 8.5 and should be used to improve the security posture of a Department of Defense (DOD) web server and its associated websites.

This document is meant for use in conjunction with the Enclave, Network Infrastructure, Application Security and Development, Windows 2012 R2 Server/Windows 8.1, and other appropriate operating system STIGs. Guidance for deployment of web servers within the DOD intranet and the Demilitarized Zone (DMZ) will be governed by the appropriate Network Infrastructure STIG provided by the Defense Information Systems Agency (DISA). This STIG has been developed based on the Web Server SRG guidance, which was published as guidance to comply with applicable NIST SP 800-53 cybersecurity controls.

This guidance is scoped to the Web Server role of Microsoft's Windows Server 2012 R2/Windows 8.1, using IIS 8.5. While no other server role or OS will be addressed, Windows Server 2012 does include .NET Framework 4.5 by default and this STIG requires .NET Framework 4.5 use for enabling specific security settings such as session state.

There are multiple STIG packages for IIS 8.5, one for IIS 8.5 server-related requirements and one for IIS 8.5 website-related requirements. Both STIGs must be applied to an IIS 8.5 web server. The individual packages are:

- IIS 8.5 Server STIG.
- IIS 8.5 Site STIG.

1.2 Authority

Department of Defense Instruction (DODI) 8500.01 requires that "all IT [information technology] that receives, processes, stores, displays, or transmits DOD information will be […] configured […] consistent with applicable DOD cybersecurity policies, standards, and architectures." The instruction tasks that DISA "develops and maintains control correlation identifiers (CCIs), security requirements guides (SRGs), security technical implementation guides (STIGs), and mobile code risk categories and usage guides that implement and are consistent with DOD cybersecurity policies, standards, architectures, security controls, and validation procedures, with the support of the NSA/CSS [National Security Agency/Central Security Service], using input from stakeholders, and using automation whenever possible." This document is provided under the authority of DODI 8500.01.

Although the use of the principles and guidelines in these SRGs/STIGs provides an environment that contributes to the security requirements of DOD systems, applicable NIST SP 800-53 cybersecurity controls must be applied to all systems and architectures based on the Committee on National Security Systems (CNSS) Instruction (CNSSI) 1253.

1.3 Vulnerability Severity Category Code Definitions

Severity Category Codes (referred to as CAT) are a measure of vulnerabilities used to assess a facility or system security posture. Each security policy specified in this document is assigned a Severity Category Code of CAT I, II, or III.

Table 1-1: Vulnerability Severity Category Code Definitions

	DISA Category Code Guidelines
CAT I	Any vulnerability, the exploitation of which will **directly and immediately** result in loss of Confidentiality, Availability, or Integrity.
CAT II	Any vulnerability, the exploitation of which **has a potential** to result in loss of Confidentiality, Availability, or Integrity.
CAT III	Any vulnerability, the existence of which **degrades measures** to protect against loss of Confidentiality, Availability, or Integrity.

1.4 STIG Distribution

Parties within the DOD and federal government's computing environments can obtain the applicable STIG from the DOD Cyber Exchange website at https://cyber.mil/. This site contains the latest copies of STIGs, SRGs, and other related security information. Those without a Common Access Card (CAC) that has DOD Certificates can obtain the STIG from https://public.cyber.mil/.

1.5 SRG Compliance Reporting

All technical NIST SP 800-53 requirements were considered while developing this STIG. Requirements that are applicable and configurable will be included in the final STIG. A report marked Controlled Unclassified Information (CUI) will be available for items that did not meet requirements. This report will be available to component authorizing official (AO) personnel for risk assessment purposes by request via email to: disa.stig_spt@mail.mil.

1.6 Document Revisions

Comments or proposed revisions to this document should be sent via email to the following address: disa.stig_spt@mail.mil. DISA will coordinate all change requests with the relevant DOD organizations before inclusion in this document. Approved changes will be made in accordance with the DISA maintenance release schedule.

1.7 Other Considerations

DISA accepts no liability for the consequences of applying specific configuration settings made on the basis of the SRGs/STIGs. It must be noted that the configuration settings specified should be evaluated in a local, representative test environment before implementation in a production environment, especially within large user populations. The extensive variety of environments makes it impossible to test these configuration settings for all potential software configurations.

For some production environments, failure to test before implementation may lead to a loss of required functionality. Evaluating the risks and benefits to a system's particular circumstances and requirements is the system owner's responsibility. The evaluated risks resulting from not applying specified configuration settings must be approved by the responsible AO. Furthermore, DISA implies no warranty that the application of all specified configurations will make a system 100 percent secure.

Security guidance is provided for the DOD. While other agencies and organizations are free to use it, care must be given to ensure that all applicable security guidance is applied at both the device hardening level and the architectural level due to the fact that some settings may not be configurable in environments outside the DOD architecture.

1.8 Product Approval Disclaimer

The existence of a STIG does not equate to DOD approval for the procurement or use of a product.

STIGs provide configurable operational security guidance for products being used by the DOD. STIGs, along with vendor confidential documentation, also provide a basis for assessing compliance with cybersecurity controls/control enhancements, which supports system assessment and authorization (A&A) under the DOD Risk Management Framework (RMF). Department of Defense AOs may request available vendor confidential documentation for a product that has a STIG for product evaluation and RMF purposes from disa.stig_spt@mail.mil. This documentation is not published for general access to protect the vendor's proprietary information.

AOs have the purview to determine product use/approval in accordance with (IAW) DOD policy and through RMF risk acceptance. Inputs into acquisition or pre-acquisition product selection include such processes as:

- National Information Assurance Partnership (NIAP) evaluation for National Security Systems (NSS) (https://www.niap-ccevs.org/) IAW CNSSP #11.
- National Institute of Standards and Technology (NIST) Cryptographic Module Validation Program (CMVP) (https://csrc.nist.gov/groups/STM/cmvp/) IAW Federal/DOD mandated standards.
- DOD Unified Capabilities (UC) Approved Products List (APL) (https://www.disa.mil/network-services/ucco) IAW DODI 8100.04.

2. ASSESSMENT CONSIDERATIONS

2.1 Product Overview

IIS 8.5 contains several components and modules performing functions to support application and web server roles in a Windows 2012 R2 or Windows 8 environment:

- Protocol listeners, such as HTTP, receive requests specific to the protocol and send the requests to IIS, which processes them and sends responses back to the requesting client.
- IIS supports protocols used by applications and services other than HTTP through the use of Windows Communication Foundation (WCF).
- Some new features in IIS 8.5 include:
  - Enhanced logging capabilities from request/response headers.
  - Ability to send logging to Event Tracing for Windows (ETW).
  - Dynamic website activation.
  - Ability to suspend idle worker process rather than terminating it.
  - Automatic certificate rebind when the certificate is renewed.

2.2 Performing a Web Server Assessment

Web servers host one or more websites and/or applications.

The IIS 8.5 Server STIG must be used to assess the web server itself. The web server is also subject to compliance with other STIGs, including but not limited to the Windows Operating System STIG, the Internet Explorer STIG, the applicable Application Server STIG (if being used), and the Application Security and Development STIG.

The IIS 8.5 Site STIG must be used to assess each and every hosted website on the web server being reviewed.