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

Version 1, Release 1

12 September 2017

Developed by DISA for the DoD

Trademark Information

TABLE OF CONTENTS

Page

1. INTRODUCTION 1

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

2. ASSESSMENT CONSIDERATIONS 5

2.1 Product Overview 5
2.2 Web Server and Site Definition 5
2.3 Web Server and Site Topology 5
2.4 Performing a Web Server Assessment 5
2.5 IIS 8.0 guidance 6

LIST OF TABLES

Page

Table 1-1: Vulnerability Severity Category Code Definitions 2

1. INTRODUCTION

1.1 Executive Summary

This Internet Information Services (IIS) 8.5 Overview is a published document to provide an overview of the IIS 8.5 Server and Site Security Technical Implementation Guides (STIGs) 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 document is a requirement for all DoD-owned information systems and DoD-controlled information systems operated by a contractor and/or other entity on behalf of the DoD that receive, process, store, display, or transmit DoD information, regardless of classification and/or sensitivity. These requirements are designed to assist Security Managers (SMs), Information System Security Managers (ISSMs), Information System Security Officers (ISSOs), and System Administrators (SAs) with configuring and maintaining security controls. This guidance supports DoD information system design, development, implementation, and certification and accreditation efforts but is restricted to policies and configurations specific to web servers and sites.

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. IIS 8.0 guidance can be found in section 2.5.

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
- IIS 8.5 Overview

1.2 Authority

DoD Instruction (DoDI) 8500.01 requires that "all IT that receives, processes, stores, displays, or transmits DoD information will be […] configured […] consistent with applicable DoD cybersecurity policies, standards, and architectures" and tasks that Defense Information Systems Agency (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, 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 need to 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 Information Assurance Support Environment (IASE) website. This site contains the latest copies of any STIGs, SRGs, and other related security information. The address for the IASE site is http://iase.disa.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 For Official Use Only (FOUO) will be available for those 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 Authorizing Official. 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 Department of Defense. While other agencies and organizations are free to use it, care must be given to ensure that all applicable security guidance is applied both at the device hardening level as well as the architectural level due to the fact that some of the settings may not be able to be configured 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). DoD Authorizing Officials (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 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) (http://www.niap-ccevs.org/) IAW CNSSP #11
- National Institute of Standards and Technology (NIST) Cryptographic Module Validation Program (CMVP) (http://csrc.nist.gov/groups/STM/cmvp/) IAW Federal/DoD mandated standards
- DoD Unified Capabilities (UC) Approved Products List (APL) (http://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 Web Server and Site Definition

A web server is an automated information system that manages one or more websites by passing or serving up web pages to an Internet browser such as Google Chrome, Mozilla Firefox, or Microsoft Internet Explorer. This document is only applicable to web servers and sites.

2.3 Web Server and Site Topology

Web server and sites operating within the DoD are segregated as one of the many hardening initiatives in order to protect the DoDIN. The approach to meet this initiative is to quarantine public-facing applications and to protect them. Additionally, protections are built into the architecture to segregate restricted and unrestricted applications from private applications.

If an IIS 8.5 web server only hosts websites where all data and content has been deemed as publicly releasable by the local Public Affairs Office (PAO) and ISSO, the server is a public web server.

If an IIS 8.5 web server hosts websites where data is mixed between private and publicly releasable, the server must be protected as a private web server.

2.4 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.

Consult the IIS 8.5 Overview, packaged separately from the STIGs, for more details.

2.5 IIS 8.0 guidance

This IIS 8.5 guidance should be used for IIS 8.0 web servers as well.

The following IIS 8.5 features are not supported by IIS 8.0 and would be Not Applicable in an IIS 8.0 environment. All other IIS 8.5 guidance applies to the IIS 8.0 web server.

- Enhanced Logging
  - Provides ability to log custom fields
  - STIG IDs in 8.5 relating to Enhance Logging
    - IISW-SV-000102
    - IISW-SV-000110
    - IISW-SV-000111
    - IISW-SI-000205
    - IISW-SI-000209
    - IISW-SI-000210
- Ability to log to ETW (Event Tracing for Windows)
  - Provides ability to log to ETW
  - STIG IDs in 8.5 relating to logging to ETW
    - IISW-SV-000103
    - IISW-SI-000206
- Idle Worker Process timeout
  - Provides ability to configure an idle worker process to Terminate or Suspend
    - Default is Terminate
    - Related STIG IDs configure timeouts
  - STIG IDs in 8.5 relating to Idle Worker Process timeout
    - IISW-SI-000235
    - IISW-SI-000257