



ORACLE HTTP SERVER (OHS) 12.1.3 SECURITY TECHNICAL IMPLEMENTATION GUIDE (STIG) OVERVIEW

Version 2, Release 3

30 January 2025

Developed by Oracle and 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 2
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. GENERAL SECURITY REQUIREMENTS 4

2.1 Supported Releases and Applicability of STIG across OHS Versions 4
2.2 Applicability of STIG across Version and Configurations 4
2.3 Certifications 4
2.4 Patches 5
2.5 Additional Products 5

LIST OF TABLES

Page

Table 1-1: Vulnerability Severity Category Code Definitions 2

1. INTRODUCTION

1.1 Executive Summary

The Oracle HTTP Server 12.1.3 Security Technical Implementation Guide (STIG) is a published document that can be used to improve the security posture of a Department of Defense (DOD) web server and its associated web sites. It is a requirement for all DOD-administered systems and all systems connected to DOD networks. It is important to note that while much of this STIG is applicable to other versions of Oracle HTTP Server, it is specific to version 12.1.3 and a standalone configuration on the Unix/Linux platforms.

This document is meant for use in conjunction with the Enclave, Network Infrastructure, Application Security and Development, and other appropriate operating system (OS) 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 DISA.

The web server must be configured to protect classified, unclassified, and/or restricted data, such as Personally Identifiable Information (PII), as well as data approved for public release. Immediate risks inherent to this role are external attacks and accidental exposure. Although security controls and infrastructure devices (such as firewalls, intrusion detection systems, and baseline integrity checking tools) offer some defense against malicious activity, security for web servers is best achieved through implementing a comprehensive defense-in-depth strategy. This strategy should include, but is not limited to, server configuration to prevent system compromise; operational procedures for posting data to avoid accidental exposure; proper placement of the server within the network infrastructure; and the allowance or denial of Ports, Protocols, and Services (PPS) used to access the web server.

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 system design, development, implementation, certification, and accreditation efforts.

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

Category	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.
- DODIN Approved Products List (APL) (https://aplits.disa.mil/processAPList.action) IAW DODI 8100.04.

2. GENERAL SECURITY REQUIREMENTS

2.1 Supported Releases and Applicability of STIG Across OHS Versions

The releases of Oracle HTTP Server supported at the time of this writing are 11.1.1.7, 11.1.1.9, 12.1.2, and 12.1.3. Please reference the following for updated support information and dates:

- Oracle Lifetime Support Policy for Oracle Fusion Middleware (www.oracle.com/us/support/library/lifetime-support-middleware-069163.pdf).
- My Oracle Support (support.oracle.com) Notes 1290894.1 and 1933372.1.

2.2 Applicability of STIG Across Version and Configurations

As previously stated, it is important to note that while much of this STIG is applicable to other versions of Oracle HTTP Server, it is specific to version 12.1.3 and the Standalone Domain configuration on the UNIX/Linux platforms. For a description of Standalone Domain configuration, read section 1.4 of the Oracle Fusion Middleware – Administering Oracle HTTP Server 12c (12.1.3) guide at https://www.oracle.com/us/assets/lifetime-support-middleware-069163.pdf and pages 8-22 of Oracle HTTP Server 12cR1 - Technical Overview located at www.oracle.com/technetwork/middleware/webtier/learnmore/ohs12c-technical-paper-2209482.pdf.

Further, while Oracle HTTP Server 12.1.3 can support the hosting of a wide variety of sites and applications, it is predominately configured with the Oracle Fusion Middleware (e.g., WebLogic) family of products, Oracle REST Data Services, Oracle Enterprise Manager, or Oracle Fusion Applications as a load balancer or proxy. It is also often configured to support Oracle APEX or other mod_plsql applications. These uses, along with the serving of static content, are the focus of this STIG. To that end, this STIG recommends the removal of many modules from the default installation.

With respect to APEX and mod_plsql applications, it should be noted that mod_plsql is deprecated in Oracle HTTP Server 12.1.3, and the statement of direction is to migrate these applications to Oracle REST Data Services.

2.3 Certifications

In an effort to reduce compatibility issues with other components of a system, Oracle provides the Oracle Fusion Middleware Supported Systems Configuration page (www.oracle.com/technetwork/middleware/ias/downloads/fusion-certification-100350.html). This provides certification information for Fusion Middleware 12c (12.1.3), which includes Oracle HTTP Server 12.1.3. Specifically, you can identify which operating systems and JDKs that Oracle HTTP Server will run on as well as the browsers, databases, Fusion Middleware, and other products that have been certified with it.

2.4 Patches

Oracle releases collections of security fixes known as Critical Patch Updates (CPUs) on a quarterly basis. As an administrator, it is your responsibility to apply these patches soon after their release. To find the applicable CPU (www.oracle.com/technetwork/topics/security/alerts-086861.html#CriticalPatchUpdates) for OHS 12.1.3, locate the latest CPU and work through the Fusion Middleware sections until finding patches that apply to the "Oracle HTTP Server 12.1.3 home". Note: Depending on the configuration and products used, patches associated with "Oracle Java SE home" "Oracle WebLogic Server Proxy Plug-ins home" may also be applicable.

2.5 Additional Products

Although Oracle HTTP Server 12.1.3 can be configured to satisfy a substantial set of the Web Server SRG requirements, there are third-party products available that can be leveraged to satisfy some of the requirements that the product by itself does not satisfy. In addition, the use of these third-party products may provide benefits beyond the native capabilities of Oracle HTTP Server itself or allow for configurations more typical to today's system implementations. Specifically, products such as Oracle Enterprise Manager and Oracle Identity and Access Management Suite could potentially be implemented to achieve greater compliance with this STIG and provide additional operational benefits to your organization.