



POSTGRESQL 9.X SECURITY TECHNICAL IMPLEMENTATION GUIDE (STIG) OVERVIEW

Version 2, Release 4

24 January 2024

Developed by Crunchy Data Solutions, Pivotal Software, 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 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 Security Assessment Information 4

3. CONCEPTS AND TERMINOLOGY CONVENTIONS 5

LIST OF TABLES

Page

Table 1-1: Vulnerability Severity Category Code Definitions 2

1. INTRODUCTION

1.1 Executive Summary

The PostgreSQL 9.x on Red Hat Enterprise Linux Security Technical Implementation Guide (STIG) is published as a tool to improve the security of Department of Defense (DOD) information systems. This document is meant for use in conjunction with other STIGs such as the Enclave, Network Infrastructure, Secure Remote Computing, and appropriate Operating System (OS) STIGs. It is based on the Database Security Requirements Guide (SRG) Version 2 Release 6, which in turn derives its cybersecurity controls from National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53, Revision 4.

PostgreSQL (also known simply as Postgres) is an open-source, community-developed relational database management system, supported by the PostgreSQL Global Development Group. That body permits and encourages the modification, extension, and redistribution of its base product. One extension of importance to this STIG is pgAudit, also open-source and developed by a parallel organization.

This STIG requires that the product be deployed on Red Hat Enterprise Linux (RHEL) to enable the use of NIST-certified cryptographic modules. While it can run and use cryptography on many versions of Linux, UNIX, and Windows, to guarantee that certified crypto modules are used by PostgreSQL, RHEL must be the operating system.

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 Security Assessment Information

While the STIG contents are categorized as manual guidance, many entries include sample or actual code for executing the checks and fixes. Additional code is provided in the Supplemental Procedures document in the STIG package.

This guidance is but one component of a robust defense-in-depth. As noted above, it is to be used along with the applicable operating system and network STIGs to provide comprehensive coverage of pertinent vulnerabilities. It is also necessary to train administrative and general users in the importance of good security practices.

3. CONCEPTS AND TERMINOLOGY CONVENTIONS

PostgreSQL is a relational database management system (DBMS), together with associated software tools.

The typical smaller PostgreSQL deployment consists of one ***instance*** of the DBMS software servicing one or more ***databases***, which are collections of data, stored in files and managed not by the operating system (OS) alone but by the DBMS. (This contrasts with some other DBMS products, such as Oracle, which typically have one database per instance or even, in clustered installations, multiple instances per database.)

Larger PostgreSQL deployments where high availability is needed can have primary and secondary instances of the DBMS software, each running on its own server, and typically servicing a single, shared database housed on dedicated storage systems. The secondary server can be invoked to take control of the database if the primary server fails.

Databases contain ***objects***, most notably ***tables*** of data. ***Constraints*** enforce validation rules on table contents. ***Indexes*** support performance tuning by providing faster lookup of data. Other object types include ***views, functions,*** and ***trigger procedures***, all of which enable database administrators and application developers to augment the functionality of the database. Objects are grouped into ***schemas***, which can be used both for ease of understanding and for security management.

Access to objects is controlled by PostgreSQL's security subsystem. A wide range of permissions and privileges exist, which the administrator grants to individuals' accounts, usually via group roles.

The language used for data definition, data manipulation, security management, etc., is Structured Query Language (SQL). PostgreSQL extends this declarative language with PL/pgSQL, which provides the power of a programming language within the database itself. Programs written in PL/pgSQL are known as functions and trigger procedures. Other languages can also be used to create functions and trigger procedures.

Applications communicate with PostgreSQL by sending it SQL or PL/pgSQL commands—usually known as queries. Applications can be written in any language capable of handling PostgreSQL's interface conventions. Applications may run on the same server as the DBMS but typically will run on dedicated web servers or client machines.