DBN-6300
SECURITY TECHNICAL IMPLEMENTATION GUIDE (STIG) OVERVIEW

24 July 2024

Developed by DB Networks 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 STIG Compliance Reporting 2
1.6 Document Revisions 2
1.7 Other Considerations 2
1.8 Product Approval Disclaimer ..... **Error! Bookmark not defined.**

2. ASSESSMENT CONSIDERATIONS 4

2.1 Security Assessment Information 4

3. CONCEPTS AND TERMINOLOGY CONVENTIONS 5

3.1 Overview 5
3.2 Architecture 5
3.2.1 Network Connection Security 6
3.2.2 Device Configuration 6

LIST OF TABLES

Page

Table 1-1: Vulnerability Severity Category Code Definitions 2

1. INTRODUCTION

1.1 Executive Summary

The DB Networks DBN-6300 Security Technical Implementation Guide (STIG) provides the technical security policies, requirements, and implementation details for applying security concepts to the DBN-6300 appliance management, backplane, and traffic inspection functions. The STIG is a package of two STIGs, which together assess the security posture of the device management, backplane, and traffic inspection functions of the appliance.

The DB Networks DBN-6300 Intrusion Detection and Prevention System (IDPS) STIG provides the technical security policies, requirements, and implementation details for applying security concepts to the Structured Query Language (SQL) injection attack detection functions of the DBN-6300 Intrusion Detection System (IDS). The DB Networks DBN-6300 Network Device Management (NDM) STIG provides the technical security policies, requirements, and implementation details for applying security concepts to the DBN-6300 management and backplane functions.

The DBN-6300 is an application layer Intrusion Detection System (IDS) that inspects the network communications traffic to detect zero-day SQL injection attacks. Traffic is inspected using behavior analysis techniques only; thus, the device is recommended for use in the architecture in front of the database tier and after the site's perimeter IDPS solution, which is typically signature based. The device is installed as a passive (bump-in-the-wire) device on the network. Administrators can use the reporting feature on the system to gain insight into what types of SQL attacks are being detected and what hidden SQL databases may be installed on the network and may be providing an attack vector for intruders. The DBN-6300 is available as a 2U appliance as well as a virtual machine.

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 STIG 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

A security assessment of the DBN-6300 must ensure both the network backplane and the IDS functions are secured. The DB Networks DBN-6300 NDM STIG contains requirements that address the management and backplane functions of the system and must be used in conjunction with the DB Networks DBN-6300 IDPS STIG.

This STIG has procedures that are intended to provide appropriate evaluation and remediation functions for organizations and locations deploying IDS for Database systems. Requirements not included in this DBN-6300 STIG may be addressed outside the scope of this document. Some policies outside of this document are set by DOD to be overarching, applying to all organizations and information systems. In some cases, DOD has determined that policy should not be set at the Enterprise level. The guidance in this STIG addresses controls to be set by all organizations and locations in support of IDS for Database systems.

3. CONCEPTS AND TERMINOLOGY CONVENTIONS

3.1 Overview

The DBN-6300 is an appliance or virtual machine that passively monitors all incoming traffic traversing the network tier where it is installed to detect SQL database injection attacks. Through the learning of normal application behaviors over a specified timeframe, and the subsequent construction of application behavioral models, the DBN-6300 provides the capability to detect SQL injection attacks with a high degree of accuracy and a false positive rate several orders of magnitude below that of signature-based systems. Upon initial installation, the system scans for existing SQL databases that are installed on the network segment. This database discovery feature allows an organization to spot rogue databases. These hidden/rogue databases can represent a considerable security risk as they are typically unmanaged, unlicensed, and/or unregulated.

Common SQL injection attacks are structural in the sense that the structure and meaning of a SQL statement is altered, typically by the insertion of new text. To detect such insertions, during the learning phase, the DBN-6300 builds models not only of SQL statements transmitted to the database but also of the ways in which those statements relate to each other. These models are based on the textual, lexical, syntactic, and semantic structures of the statements.

DB Networks refers to the DBN-6300 as a Core IDS to indicate that it monitors all SQL traffic coming into the database tier and monitors that traffic for abnormal application behavior. Abnormal application behavior consists of any and all application behavior that creates or attempts to create behavior that was not originally intended by the application programmers. Upon detection of abnormal application behavior, an event is created and sent to the site's event monitoring system, which can then be configured to notify responsible security personnel for appropriate action.

To determine whether those statements are a potential attack, the system compares incoming database statements to learned profiles. This is done by running the statements and responses through a series of algorithms, each of which generates one or more scores against its internal model of the application. A master scoring algorithm evaluates the scores from each model's perspective and creates a single master score, and events are categorized as "Certain", "Likely", or "Possible". Each level represents the degree of confidence, from the system's perspective, that a statement execution is an actual attack.

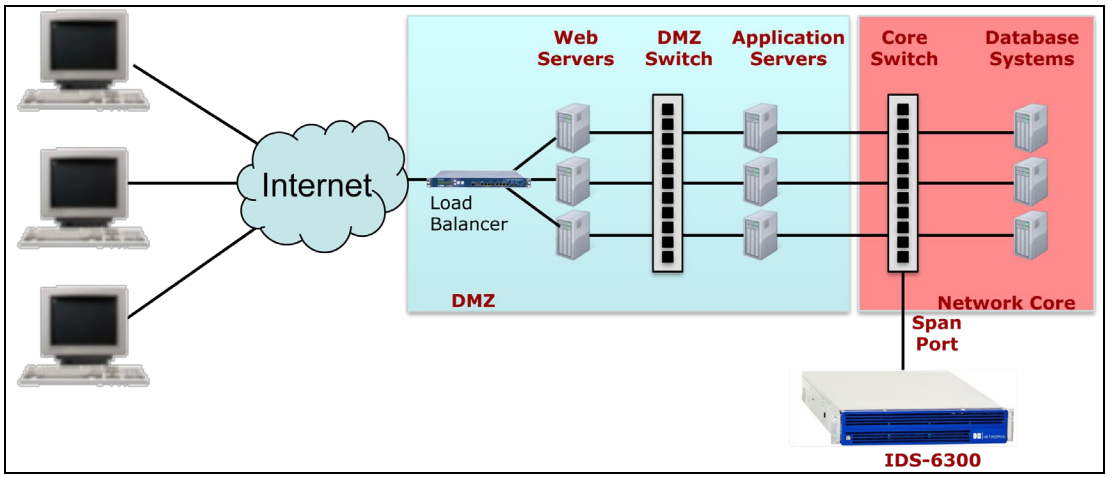
Additional capability can easily be leveraged with a high degree of effectiveness, and that is the ability to play back a network capture file (PCAP) through the DBN-6300. This will cause DBN-6300 to behave in exactly the same manner as it would have if it had been sitting in the same location as that of the traffic capture. This is useful in environments where continuous monitoring is not required and/or the permanent attachment on an IDS is impractical.

3.2 Architecture

To maximize protection of the database tier, the DBN-6300 must be architecturally placed at the internal boundary between the application and database tier, as shown in Figure 3.1. However, since hidden databases are a common issue on an enterprise network, the appliance may also be placed at the perimeter to discover and continuously or periodically monitor for rogue SQL databases. In

either case, the DBN-6300 cannot be used as the site's primary IDPS solution at the perimeter since it monitors only inbound traffic and is special to monitor only SQL statements. All inbound and outbound communications traffic, including database traffic, must first be inspected by the perimeter firewall and IDPS in compliance with DOD policy.

Figure 3-1: DBN-6300 Example of Network Placement



3.2.1 Network Connection Security

Securing the DBN-6300 device from attack is also important because IDSs are often targeted by attackers. If an attacker can compromise an IDS, it can be rendered useless in detecting subsequent attacks against other hosts. The appliance must be installed in stealth mode, without IP addresses assigned to its monitoring interfaces, and using a mirrored, Switch Port Analyzer (SPAN) port. Stealth mode improves the security of the IDS sensors because it prevents other hosts from initiating connections to them. This conceals the sensors from attackers and thus limits their exposure to attacks. The network interface card (NIC) connected to the SPAN port must not have any network protocol stacks bound to it. A separate network interface would then be connected to an out-of-band (OOB) network for administration and management. Stealth mode will reduce the risk of the IDS itself being attacked.

3.2.2 Device Configuration

Once connected to the production network, the DBN-6300 will begin to see database traffic as soon as the capture port or ports are enabled. Database service names will appear almost immediately and become visible through the database discovery window in the user interface (UI). Here users will discover many database service names they were unaware of, as well as all of the traffic patterns that those database services currently have. This is one of the methods that organizations use to determine which databases are being used with regularity and which are not. This allows an organization to make decisions with respect to database consolidation. Database consolidation provides a very straightforward path to reduction of the database vulnerability footprint, as well as more directly exposing unauthorized databases that were not sanctioned and that represent major security holes in that organization. Further, as the system is operating in its

normal production mode, any new database services that appear will create an alert on the system, demanding immediate attention and possible remediation.