

UNCLASSIFIED



# **BROADCOM CONTENT ANALYSIS SYSTEM (CAS) SECURITY TECHNICAL IMPLEMENTATION GUIDE (STIG) OVERVIEW**

**Version 1, Release 1**

**26 August 2026**

**Developed by Broadcom and DISA for the DoW**

UNCLASSIFIED

### **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     |
|------------------------------------------------------------|----------|
| <b>1. INTRODUCTION.....</b>                                | <b>1</b> |
| 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        |
| <b>2. GENERAL SECURITY REQUIREMENTS.....</b>               | <b>4</b> |
| 2.1 FIPS Mode Initialization and System Impact.....        | 4        |
| 2.1.1 Pre-Execution Prerequisites.....                     | 4        |
| 2.1.2 Post-Execution Recovery.....                         | 4        |

LIST OF TABLES

|                                                                   | Page |
|-------------------------------------------------------------------|------|
| Table 1-1: Vulnerability Severity Category Code Definitions ..... | 1    |

## 1. INTRODUCTION

### 1.1 Executive Summary

This Broadcom Content Analysis System (CAS) Security Technical Implementation Guide (STIG) provides the technical security policies, requirements, and implementation details for applying security concepts to the Broadcom CAS network security appliance.

The Broadcom CAS is a purpose-built, high-throughput network security appliance designed to provide in-flight malware scanning and threat analysis. It integrates with network proxies (e.g., Edge SWG) via the Internet Content Adaptation Protocol (ICAP). Because it is a hardened, headless appliance rather than a general-purpose operating system, its security architecture relies heavily on strict network isolation, Role-Based Access Control (RBAC), and integration with enterprise security services.

### 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 DoW 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.            |

| Category | DISA Category Code Guidelines                                                                                                       |
|----------|-------------------------------------------------------------------------------------------------------------------------------------|
| 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 DoW 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 DoW 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](mailto: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](mailto:disa.stig_spt@mail.mil). DISA will coordinate all change requests with the relevant DoW 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 DoW. 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 DoW architecture.

## 1.8 Product Approval Disclaimer

STIGs provide configurable operational security guidance for products being used by the DoW. 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 DoW Risk Management Framework (RMF). DoW 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](mailto: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) DoW policy and through RMF risk acceptance. Inputs into acquisition or preacquisition 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/DoW mandated standards.

## 2. GENERAL SECURITY REQUIREMENTS

### 2.1 FIPS Mode Initialization and System Impact

Executing the command to enable FIPS mode triggers a complete factory reset of the appliance.

- All existing system configurations (including network interfaces, routing, and policies) will be permanently erased.
- All local user accounts and passwords will be deleted.
- All locally stored data and audit logs will be wiped.
- The system will immediately reboot to initialize the FIPS-compliant cryptographic boundaries.

#### 2.1.1 Pre-Execution Prerequisites

To prevent catastrophic loss of access or operational disruption, the following actions must be completed prior to enabling FIPS mode:

1. **Timing:** FIPS mode should ideally be enabled during the initial out-of-the-box deployment before any production configurations are applied. If FIPS mode must be enabled on an active production system, it must be performed strictly within an approved, scheduled maintenance window.
2. **Configuration Backup:** Administrators must generate and securely export a complete backup of the current system configuration.
3. **Physical/Out-of-Band Access:** Because the network configuration will be erased, SSH and Web Management access will be severed immediately upon reboot. Administrators must have a direct physical serial console connection (or out-of-band management console access) established to reconfigure the base IP addresses and management routing after the system reboots.

#### 2.1.2 Post-Execution Recovery

Following the reboot into FIPS mode, administrators must use the serial console to re-establish network connectivity before restoring the backed-up configurations and continuing with the remaining STIG compliance checklist.