FORESCOUT COUNTERACT SECURITY TECHNICAL IMPLEMENTATION GUIDE (STIG) OVERVIEW

Version 1, Release 1

12 September 2017

Developed by ForeScout 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 DISA of any non-Federal entity, event, product, service, or enterprise.

TABLE OF CONTENTS

Page

LIST OF TABLES

Page

1. INTRODUCTION

1.1 Executive Summary

The ForeScout CounterACT Security Technical Implementation Guide (STIG) provides the technical security policies, requirements, and implementation details for applying security concepts to the CounterACT Enterprise Manager (EM) and CounterACT appliance. The STIG is a package of two STIGs that together ensure the secure implementation of the Network Device Management (NDM) function and the Network Access Control (NAC) traffic services.

ForeScout CounterACT provides NAC and threat protection for the enterprise. CounterACT integrates with compatible switches and other network infrastructure equipment to enforce DoD access control policies for detected devices. Devices may be managed or unmanaged and the assessment policies are largely vendor-specific since CounterACT has a large network product database. CounterACT also provides access control network services that are user aware. These services allow trusted users who are using validated endpoints configured in compliance with the organization's security policies to remain productive while protecting critical network resources and sensitive data. CounterACT implements functions such as traffic filtering, authentication, access, and authorization functions based on computer and user privileges. However, the directory service (e.g., Active Directory or LDAP) must not be installed on CounterACT, particularly if the gateway resides on the untrusted zone of the Enclave. Although CounterACT can be upgraded and configured with features such as guest access and the ability to protect network resources from threats such as malware and worms, these upgrades are not within the scope of this document and these capabilities.

An Enterprise Manager, as well as at least one appliance, should be implemented to meet redundancy and centralization requirements. The Enterprise manager allows the organization to meet centralized management requirements and provides more robust management and auditing tools. Audit tools for CounterACT include the Web Portal and Enterprise Management software. Both tools require authenticated access, although the Web Portal can only work with password access and thus must only be used from the management VLAN and management station. Additionally, because CounterACT can also be configured for malware threat protection, guest access, and other capabilities, a complete security assessment requires assessing all modules integrated into the specific DoD implementation. Each security review must include the ForeScout CounterACT NDM STIG and ForeScout CounterACT ALG STIG, at a minimum, regardless of the role in the network architecture or modules installed. Since product STIGs are not available for all configurations/modules, use of existing generic technology STIGs may be required to secure these functions. This STIG focuses on the hardware-based CounterACT platform. The CounterACT virtual platform was not tested and is not part of the scope of this STIG.

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

2.1 Security Assessment Information

A security assessment of the ForeScout CounterACT must consist of a review of device hardening and the access control and threat protection function. Thus, the ForeScout CounterACT NDM STIG and the ForeScout CounterACT ALG STIG are required for all security reviews.

2.2 Security Plug-Ins

The following list of core security plug-ins is provided as a reference for security assessors and installers. Plug-ins beyond those listed below have not been assessed for use in DoD and are not approved as part of the core CounterACT operations in DoD.

- DHCP Classifier: The latest DHCP fingerprints for device classification.
- Hardware Watchdog: Automatically restarts a services if it stops.
- HPS Applications: In-depth discovery and management of software and applications on Windows endpoints.
- HPS Inspection Engine: Inspect, manage, remediate, and control Windows endpoints.
- HPS NIC Vendor DB: Map Network Interface Controllers (NIC) to their vendors based on their MAC address.
- HPS Vulnerability DB: Vulnerability Database; updates soon after they are released from Microsoft.
- Macintosh-Linux Property Scanner: Inspect, manage, remediate, and control Mac and Linux endpoints. Should be disabled if not in use.
- NBT Scanner: Obtains the user logged on to a given host and the MAC address of that host and also discovers the NetBIOS name of the host.
- Reports: Generates reports.
- Switch: Switch integrations.
- Syslog: Send and receive Syslog messages. Should be disabled if not in use.
- Technical Support: Automatically analyze an extensive range of log files on CounterACT and optionally send them to the ForeScout support team for further investigation.
- User Directory: Resolves endpoint user details and performs endpoint authentication via authentication and directory servers.
- Wireless: Wireless Controller and Access Point integrations. Should be disabled if not in use.