MICROSOFT (MS) WINDOWS 2012 SERVER DOMAIN NAME SYSTEM (DNS) SECURITY TECHNICAL IMPLEMENTATION GUIDE (STIG) OVERVIEW

Version 1, Release 8

26 January 2018

Developed by DISA for the DoD

Trademark Information

TABLE OF CONTENTS

Page

LIST OF TABLES

Page

1. INTRODUCTION

1.1 Executive Summary

This Microsoft Windows 2012 Domain Name System (DNS) Security Technical Implementation Guide (STIG) is published as a tool to secure Microsoft Windows 2012 DNS implementations.

This STIG will be used for all Windows 2012/2012 R2 DNS servers, whether Active Directory-integrated, authoritative file-backed DNS zones, a hybrid of both, or as a recursive caching server. This STIG should also be used for Windows 2012 DNS servers being used as a secondary name server for zones whose master authoritative server is non-Windows.

The direction is to ensure Windows 2012 DNS data's authentication and integrity through the means of applying DNS Security Extensions (DNSSEC), specified by the Internet Engineering Task Force (IETF) Requests for Comment (RFC4641, RFC5011, RFC5155, RFC4033, RFC4034, RFC4035, and RFC3833) and as outlined in the NIST Special Publication (SP) 800-81, "Secure Domain Name System (DNS) Deployment Guide". In addition, the NIST SP 800-81 rev 2, "Secure Domain Name System (DNS) Deployment Guide" has been a resource in the development of this Windows 2012 DNS STIG.

As the DNS Server service in Windows Server 2012 has greatly enhanced support for DNSSEC, these STIG settings are required for all Windows 2012/2012 R2 DNS implementations.

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 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.

1.6 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.

1.7 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 CONSIDERATIONS

2.1 Security Assessment Information

This Microsoft Windows 2012 DNS STIG is intended to be used in conjunction with the Windows 2012 Active Directory and Domain Controller STIGs, which are separate STIGS; this Microsoft Windows 2012 DNS STIG does not replace those STIGs.

Checks and Fixes verbiage may include DNS Manager console instructions, instructions to be executed at a command line prompt, or instructions to be executed at a PowerShell prompt. PowerShell commands must be run from either a Windows 8 or Windows 2012 or higher operating system in order to assure validity of the results since some PowerShell commands have been released only for the Windows 8/Windows 2012 operating systems.

While there are multiple methods that can be used to both validate and fix a setting, generally only one is listed for each in the STIG.

Other methods listed for a Fix can feasibly be used to reach the same end result of remediating the vulnerability associated with the requirement.

There are multiple requirements in the STIG that are deemed compliant by the very nature of the zones being signed with DNSSEC and by configuring IPSec for DNS servers.

Microsoft hotfix KB2956577 must be applied to Windows 2012 R2 DNS servers in order to meet Diagnostic logging and auditing requirements in the STIG.

3. CONCEPTS AND TERMINOLOGY CONVENTIONS

3.1 How DNSSEC Secures DNS Data

DNSSEC uses asymmetric Public/Private key cryptography to provide Digital Signature Validations. Once a zone is signed with DNSSEC, every individual DNS Resource Record in a zone is accompanied by Delegation Signer (DS) Resource Record (RR) and a Resource Record Signature (RRSIG).

- The DS RR is a Hash value of that record. The RRSIG record is an encrypted copy of the Hash value (encrypted using the DNS Server's private key stored on the DNS server).
- When a resolver, client or caching server, requests to send a query to a DNSSEC-enabled DNS server, the query answer is returned accompanied by the DS and RRSIG.
- The resolver then uses the public key (DNSKEY) obtained from the DNS server to decrypt the RRSIG record and then compares the Hash value in the DS.
- If the result of the DNSSKEY decryption on the RRSIG matches the DS, the DNS data is approved as a valid source.

Before DNS signatures can be validated, however, all systems must trust a common authority. The authority is called the Trust Anchor. The common DNS Trust Authority is the DNS Root Server (i.e., .com, .edu, .org, .mil, etc.). Any child zones/domains of these Trust Points (i.e., disa.mil) will be vouched for by this authority if not individually signed. As of May 5, 2012, all Internet Root DNS Servers have been digitally signed.

A caching DNS server will validate DNS query requests from clients if it is pointed to a Trust Anchor or Trust Point and the Trust Anchor/Trust Point has a stored copy of the Public keys for the DNS zone requested in the query, or from a parent zone.

Within the DoD, the Enterprise Resolving Server (ERS) holds the Public keys for external DNS zones so that when internal DoD DNS caching servers/clients forward queries to the ERS, this DNSSEC validation occurs. DNSSEC validation occurs even if a client is not DNSSEC-aware. While Windows 2008 first introduced some DNSSEC capability, the DNS Server service in Windows Server 2012 has greatly enhanced support for DNS Security Extensions (DNSSEC).

FRAGO1 to TASKORD 11-0410-2 specified that all CC/S/FAs must implement DNSSEC on their respective second-level .mil domain by 1 May 2013. DNSSEC for all lower level .mil subdomains was directed to be implemented by 3 Jun 2014. This requirement is for Unclassified networks only; Classified networks are exempt from the DNSSEC requirements and those requirements may be marked N/A for such systems.

3.2 Securing DNS traffic in Windows 2012/2012 R2

3.2.1 Securing DNS query/response

Threats specific to DNS query/responses are mitigated by signing all zones with DNSSEC.

3.2.2 Blackhole name servers

Name servers configured as blackhole name servers will be treated in the STIG as a caching/forwarding name server. This will only apply if the blackhole name server has manual records added and is not otherwise authoritative for any zones.

In such an environment, clients/resolvers in the organization will point to this blackhole server for the purpose of determining whether an intended destination is blacklisted.

If an intended destination is not blacklisted, the blackhole server must then default to a forwarding or caching role and either point to another internal or DoD name server for completing the external recursive lookup or point to the DISA ERS for external recursive lookup.

All STIG requirements referencing caching name servers do apply to a blackhole name server.

Since the server will not be authoritative for any zone, DNSSEC is not required on a blackhole name server.

3.2.3 Securing DNS zone transfers, dynamic updates, and DNS Notify

Threats specific to DNS zone transfers, dynamic updates, and DNS Notify are mitigated by using encryption when transmitting server-to-server, client-to-server, or server-to-client DNS information. This encryption can be accomplished by using Transaction SIGnature (TSIG), SIG(0), or IPSec. Windows DNS Server does not support TSIG/SIG(0), so IPSec will be required for that protection.

3.2.3.1 DNS zone transfers and DNS Notify

Although the AD replication process provides a means for a certain level of securing the transmission of the DNS information between DNS servers in a 100% AD-integrated environment, Windows servers, whether in an AD-integrated, non-AD-integrated, or mixed configuration require a means for securing the server-to-server communications.

As per Microsoft in the following Knowledge Base article, zone transfers can be secured using IPSec. Since Windows Server 2012 and Windows Server 2012 R2 do not support Transaction Signature (TSIG) for zone transfers, IPSec will be required for that protection.

http://technet.microsoft.com/en-us/library/dn593674.aspx#zone_transfers

Certificate-based authentication can be used to establish an IPSec session between DNS servers. Each endpoint must present a certificate to prove its identity. This method requires that certificates are created and configured on all DNS servers that participate in zone transfers for DNSSEC-signed zones.

Procedures for deploying certificates for DNS server authentication can be found at the following Microsoft link:

http://technet.microsoft.com/en-us/library/dn593680.aspx

Procedures for configuring IPSec between DNS servers can be found at the following Microsoft link:

http://technet.microsoft.com/en-us/library/dn593634.aspx

3.2.3.2 Dynamic updates

Microsoft has implemented a proprietary version of GSS-TSIG into their Dynamic Update function. When the Windows Server 2012 DNS is configured with "Secure only" for accepting Dynamic Updates, the clients must be part of the Active Directory in order for the update to the DNS to be accepted. This meets the requirements for authentication for Dynamic Updates in an AD-integrated configuration.

3.3 DNSSEC-specific enhancements in Windows 2012/2012 R2

3.3.1 Key Master Role

The Key Master is an authoritative DNS server that generates and manages signing keys for a zone that is protected with DNSSEC. The Key Master role was introduced in Windows Server 2012 for Active Directory-integrated zones. The Key Master role was introduced for file-backed multi-master zones in Windows 2012 R2.

Windows Server 2012 and R2 introduced isolation of the key management process from primary DNS servers that are not the Key Masters of a zone. The signing process can only be initiated from the Key Master; other primary servers can continue the zone signing by accessing these keys.

3.3.2 Other Enhancements

Other enhancements to DNSSEC in Windows 2012/2012 R2 included:

- Support for Active Directory-integrated DNS scenarios, including DNS dynamic updates in DNSSEC-signed zones
- Support for updated DNSSEC standards, including NSEC3 and RSA/SHA-2
- Automated trust anchor distribution through Active Directory
- Automated trust anchor rollover support per RFC 5011
- Updated user interface with deployment and management wizards
- Validation of records signed with updated DNSSEC standards (NSEC3, RSA/SHA-2)
- Easy extraction of the root trust anchor

4. GENERAL SECURITY REQUIREMENTS

Reference the “Domain Name System (DNS) Security Requirements Guide (SRG) Technology Overview” document for more background and detail on the general security requirements of Domain Name Systems.