

[Serial Number]

[Date]

[Enter Assessment Title Here.] (Draft)

If <STAKEHOLDER NAME>, wishes to create and distribute derivatives of this report (such as summaries of this report or <STAKEHOLDER NAME> commentary on the report’s recommendations), <STAKEHOLDER NAME> should (1) provide notice to CISA prior to distributing such derivatives; (2) clearly mark derivatives so that it is clear that <STAKEHOLDER NAME> created them and so that they cannot be mistaken for official CISA documents; and (3) refrain from affixing the CISA logo or DHS seal to the derivatives, unless <STAKEHOLDER NAME> has obtained written permission to do so from the CISA Office of External Affairs.

The unauthorized use of any Federal agency’s seal is governed by the U.S. Code title 18 sections 506, 701, 709 and 1017. Requests to use the CISA logo or DHS seal should be directed to [branding@cisa.dhs.gov](mailto:branding@cisa.dhs.gov), copying ciocc@cisa.dhs.gov.

Risk and Vulnerability Assessment

[Enter Assessment Title]

Risk and Vulnerability Assessment

[Serial Number]

August 27, 2021

Table of Contents

[Summary of Results 3](#_Toc52528380)

[Scope 5](#_Toc52528381)

[Methodology 5](#_Toc52528382)

[Narrative 5](#_Toc52528383)

[Attack Paths 6](#_Toc52528384)

[General recommendations 7](#_Toc52528385)

[Findings 8](#_Toc52528386)

[Appendix B: External Port Mapping 10](#_Toc52528387)

[Appendix C: Password analysis 11](#_Toc52528388)

[Appendix D: Abbreviations and Acronyms 12](#_Toc52528389)

Tables

**No table of figures entries found.**

Figures

[Figure 1: Findings Summary Table 3](#_Toc52528390)

[Figure 2: Most Frequently Cited NIST Controls 3](#_Toc52528391)

[Figure 3: NIST Cybersecurity Framework Controls 4](#_Toc52528392)

[Figure 8: Scan Results 5](#_Toc52528393)

[Figure 11: CIS Controls Based Recommendations 7](#_Toc52528394)

[Figure 12: Findings Breakdown 8](#_Toc52528395)

# Summary of Results

The Department of Homeland Security (DHS) Cybersecurity and Infrastructure Security Agency (CISA) Assessments team conducted a Risk and Vulnerability Assessment (RVA) at the request of the {Stakeholder Long Name}. ({Stakeholder Initials}). {Fed lead Name} ({Fed lead Email}) led a CISA Assessment Team remotely and on site at {Stakeholder Long Name}, USA from {External Start Date} to {Internal End Date}.

During testing CISA successfully compromised the following:

{Cisa Results}

Considering this test, CISA recommends the following high-level actions:

{Cisa Recommendations}

This report only covers the targets described within and makes no claims about the security of any system that was deemed out of scope or was not tested during this engagement.

## Findings Summary

Below is a summary table of the results from the RVA. Detailed results can be found in subsequent sections of this report.

{Table: CISA Findings}

Figure : Findings Summary Table

{CISA Findings Summary}

## NIST-Based Summary

The CISA Assessments team mapped all the findings (see [Findings](#AppA_Findings)) to applicable National Institute of Standards and Technology (NIST) controls as described in NIST Special Publication (SP) 800-53. Figure 22 illustrates the most common control families cited based on the number of findings. [Findings](#AppA_Findings) provides the complete mapping and the detailed technical description for each finding. Note that some findings may be mapped to multiple applicable NIST controls.

{NIST 800-53 Controls}

Figure : Most Frequently Cited NIST Controls

## NIST Cybersecurity Framework

RVA findings are mapped to the NIST Framework for Improving Critical Infrastructure Cybersecurity, Version 1.0, February 12, 2014, called the Cybersecurity Framework. Figure 3 illustrates the most common controls cited based on the number of findings. [Findings](#AppA_Findings) provides the complete mapping and the detailed technical description for each finding. Note that some findings may be mapped to multiple applicable NIST controls.

{NIST CSF}

Figure 3*: NIST Cybersecurity Framework Controls*

## Verified Exposures

The CISA Assessment Team evaluated four common risk exposures: Insider Threat, Phishing, Ransomware, and Data Disclosure. The exposures are assessed to verify the ability of a threat actor to take advantage of the exposure, leading to the materialized risk.

The exposure scores are calculated by a weighted average of the number of associated discovered findings over the total number of associated findings. A higher score indicates the potential for a threat actor to have a greater opportunity to take advantage of a risk exposure within {Stakeholder Long Name}’s organization. This analysis can be used to support subsequent risk analyses, such as those that prioritize risks based upon impact and likelihood of occurrence.

### Insider Threat Exposure

Insider Threat refers to the potential for an authorized user to use their access in a way that could negatively affect the organization, such as through sabotaging critical systems or exfiltrating sensitive data ([cite](https://insights.sei.cmu.edu/insider-threat/2017/03/cert-definition-of-insider-threat---updated.html)). Insider Threat exposure refers to how vulnerable the organization is to the misuse and abuse of authorized access by users.

{Insider Threat Risk Gauge}

### Phishing Exposure

Phishing is the practice of sending fraudulent emails in order to induce victims into revealing personal information or allowing access to their systems. Phishing exposure refers to how susceptible the organization is to receiving phishing emails and falling victim to a phishing campaign. Both technical factors as well as human factors can contribute to the phishing exposure of the organization. Typically a phishing attack will start with a fraudulent email trying to convince the target to either visit a site or open a malicious file that is linked in the email. Upon visiting or opening the attachment, malicious actors will obtain access to either credentials or direct access to the organization's machines. This can be a catalyst for malicious actors creating larger and more damaging attacks against the organization.

{Phishing Risk Gauge}

### Ransomware Exposure

Ransomware is malware that uses strong encryption to lock targeted files on compromised systems. Ransomware exposure refers to how vulnerable the organization is to this form of malware. Some ransomware variants have new attack strategies and exfiltrate the victim’s data before encryption. The attackers then threaten to publicly publish it online as a secondary tactic to collect a ransom payment. Ransomware attacks are mainly opportunistic and usually infect a myriad of easy targets in the hopes of collecting the highest financial reward. Infections can be automated or require manual deployments. After an attacker uses ransomware to encrypt a victim’s data, the attacker sends a ransom note demanding payment for a decryption tool to recover the data held hostage. The impact of a ransomware incident can be severe and cripple an organization with lost revenue, data loss, damaged public reputation, incident response and recovery costs, reporting costs, and data breach fines.

{Ransomware Risk Gauge}

### Data Disclosure Exposure

Data Disclosure typically refers to information that can be accessed and potentially leveraged by an attacker for additional access, weaponization against the network, or damage to the organization's reputation. Data Disclosure exposure is determined based on the quantity of disclosed data, the sensitivity of the data, and the potential access or damage that could be achieved with the data. Sensitive data can include information like usernames, passwords, private keys, or other information that can be used to progress the attack by an adversary. Disclosure of sensitive data such as PII can also harm an organization's reputation. The impact of a data disclosure incident can range from further infection of the organization's infrastructure to sensitive information being disclosed to the public.

{Data Disclosure Risk Gauge}

Scope

|  |  |  |
| --- | --- | --- |
|  | EXTERNAL | INTERNAL |
| Scope | {Short business level external scope – tech scope is in appendix.} | {Short business level internal scope – tech scope is in appendix.} |
| Scanned Hosts | {Number of External Addresses Scanned} | {Number of Internal Addresses Scanned} |
| Alive Hosts | {Number of External Hosts Identified} | {Number of Internal Hosts Identified} |

Figure : Scan Results

Methodology

CISA assessments consist of several phases, which are detailed in the subsequent sections. CISA follows the Penetration Testing Execution Standard (PTES) as the model for penetration testing activities. The standard can be found at: <http://www.pentest-standard.org>.

Narrative

The goal of CISA assessments is to identify vulnerabilities and/or weaknesses that could allow an attacker to compromise or impact the in-scope systems. This assessment provides a snapshot in time perspective on the resilience of the tested systems to threats from multiple threat actors. This assessment was conducted according to a black box methodology, with no prior knowledge of the services, hosts, or networks, unless otherwise noted.

{Narrative Sections}

Attack Paths

## {Attack Path Diagrams}

## ATT&CK

{Table: ATTACK Matrix}

General recommendations

To support the CISA Assessments team’s goal of helping stakeholders improve their security posture, the assessment team identified general recommendations based on the Center for Internet Security’s Critical Infrastructure Security (CIS) controls for mitigating the risks discovered. Figure 511 represents a high-level summary of prioritized recommended remediations and the associated findings. As always, {Stakeholder Long Name} has a much deeper understanding of its business and technical environment standards that should determine the balance of implementation.

{Table: CIS\_CSC}

Figure : CIS Controls Based Recommendations

The CISA Assessments team is available to assist with any follow-up that {Stakeholder Long Name} may need. For additional information on the CISA Assessments team’s service offerings, contact the team via email at [vulnerability\_info@cisa.dhs.gov](mailto:vulnerability@cisa.dhs.gov).

# Findings

The CISA Assessments team identified the following findings as potentially exploitable vulnerabilities that could compromise the confidentiality, integrity, and availability of the tested environment. Each finding includes a description, supporting details, and recommended steps for mitigation. The {Stakeholder Long Name} team should review the findings and recommendations for technical weaknesses, shortcomings in processes and procedures, and systemic weaknesses in overall security posture.

See [Appendix A](#AppA4_Severity) for definitions of each level of severity (Critical/High/Medium/Low/ Informational).

{Table: NCATS Detailed Findings}

# Appendix A: Severity Rating Criteria

|  |  |
| --- | --- |
| Severity | Description |
| Critical | Critical vulnerabilities pose an immediate and severe risk to the environment because of the ease of exploit and potential severe impact. Critical items are reported to the customer immediately. |
| High | Intruders may be able to exercise full control on the targeted device.  Here are examples:   * Easily exploitable vulnerabilities that can lead to complete application, system, or network compromise, such as an intruder having the ability to remotely administer files on a web server * Severe router/firewall/server misconfigurations * Worm, Trojan, or backdoor detected * Vulnerability that has tools readily available on the Internet to take advantage of it * Weak passwords for remote administration and users |
| Medium | Intruders may be able to exercise some control of the targeted device.  Here are examples:   * Disclosure of unauthorized sensitive customer information or user account information * Ability of an intruder to obtain full read access to corporate confidential information * Lack of basic logging and alerting capabilities * Antivirus misconfigurations * Untrusted networks having access to trusted networks |
| Low | The vulnerabilities discovered are items of interest but are not normally exploitable. Many low-severity items reported by security tools are not included in this report because they are often informational, unverified, or of minor risk. |
| Informational | These vulnerabilities are potential weaknesses within the system that cannot be readily exploited. These findings represent areas of which the customer team should be aware, but they do not require any immediate action. |

# APPENDIX B: Verified EXposure tables

{Table: Verified Exposures}

# Appendix C: External Port Mapping

{Table: Port Mapping}

# Appendix D: Password analysis

CISA obtained the hashed passwords for all the {Stakeholder Long Name} users during the assessment. Over the course of 24 hours CISA attempted to obtain the clear text passwords represented by the hashed values. The following is some statistical analysis of the clear text password recovered by CISA:

{Password Analysis Output}

# Appendix E: Abbreviations and Acronyms

{Table: Abbreviations and Acronyms}