

Federal Attack Surface Testing Assessment Report (Draft)

{REPORT SUBTITLE}

{ DATE }

If {Stakeholder Name}, wishes to create and distribute derivatives of this report (such as summaries of this report or {Stakeholder Name}’s 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, copying ciocc@cisa.dhs.gov.

Table of Contents

[Findings 3](#_Toc143591621)

[Attack Paths 5](#_Toc143591622)

[Appendix A: Severity Rating Criteria 5](#_Toc143591623)

[APPENDIX B: Narrative 6](#_Toc143591624)

[Appendix C: Scope 6](#_Toc143591625)

[Appendix D: External Port Mapping 6](#_Toc143591626)

[Appendix E: Abbreviations and Acronyms 7](#_Toc143591627)

Tables

[Table 1: Summary of Findings, Severity, and Mitigation Status 3](#_Toc143591628)

[Table 2: Severity Rating Descriptions 5](#_Toc143591629)

[Table 3: Open Ports and Services on External Systems 6](#_Toc143591630)

Figures

No table of figures entries found.

# Findings

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

### Severity can be used to prioritize mitigation of findings. However, {Stakeholder Name} is best equipped to develop a mitigation strategy based on business impact and priorities. Mitigation Status indicates whether a finding was mitigated during the assessment timeframe and is only adjusted when the CISA team can confidently validate that the finding was mitigated.

## Findings Summary

{Table: Findings Summary}

Table : Summary of Findings, Severity, and Mitigation Status

### See [Appendix A](#APPA) for the criteria used to determine severity (Critical/High/Medium/Low/Informational).

## Detailed Findings

{Table: Detailed Findings}

{PHISHING CAMPAIGN RESULTS}

# Attack Paths

Attack paths are used to demonstrate impact by chaining together vulnerabilities and misconfigurations to achieve a significant level of access. The sections below provide a high-level overview of attack paths that the CISA team executed during the engagement and the corresponding MITRE ATT&CK techniques that were leveraged in each attack. A detailed breakdown of each attack path can be found in the corresponding [Appendix D: Narrative](#NAR) section.

{ATTACK PATHS}

# Appendix A: Severity Rating Criteria

The severity selected for each finding during the RVA are determined using the criteria outlined below.

|  |  |
| --- | --- |
| **Severity** | **Description** |
| **• Critical** | Critical findings pose an immediate and severe threat to the environment due to ease of exploitation and significant impact. In most cases, critical findings are reported immediately, and rapid mitigation should be considered. |
| **• High** | High findings may be leveraged by an adversary to obtain full control over a targeted asset. This includes but is not limited to: easily exploitable vulnerabilities that lead to complete compromise of an application, system, or network; significant router/firewall/server misconfigurations; weak password configurations that lead to administrator account compromise; or any vulnerability that can be exploited using readily available tools leading to significant compromise of an asset. |
| **• Medium** | Medium findings may be leveraged by an adversary to obtain some control over a targeted asset. This includes but is not limited to: unauthorized disclosure of sensitive customer or user account information; unauthorized read access to sensitive business information; weak anti-virus implementation/configurations; and lack of segmentation between untrusted and trusted networks. |
| **• Low** | Low findings typically encompass items of interest that are not readily exploitable and/or do not result in compromise to confidentiality, integrity, or availability of assets. The raw data and scan reports provided by the CISA team should be reviewed for additional findings that may have been deemed low severity but were not included in this report based on the minor risk they present. Due to time constraints, the CISA team prioritizes higher risk findings and may not be able to validate lower severity findings. |
| **• Informational** | Informational findings are potential weaknesses within the environment that cannot be readily exploited. These findings represent areas that should be investigated further, but do not require immediate action or mitigation. |

Table : Severity Rating Descriptions

# APPENDIX B: Narrative

This section highlights key tools and techniques the CISA team utilized during testing and can be used to replicate the CISA team’s actions or better understand how a particular finding was identified. These actions should only be replicated by an experienced individual who thoroughly understands the functionality and risks of the tools and techniques.

{NARRATIVE SECTION}

# Appendix C: Scope

{Table: Scope}

# Appendix D: External Port Mapping

During external testing, the CISA team identified the following open ports/services on {Stakeholder Name}’s public-facing systems. It is recommended to review the data below, determine if any unnecessary ports/services are publicly accessible, and minimize the external attack surface where possible.

{Table: Port Mapping}

Table : Open Ports and Services on External Systems

# Appendix E: Abbreviations and Acronyms

{Table: Acronyms}