

**Nov 2020**

Combat Capabilities Development Command (CCDC) Data & Analysis Center (DAC) Cooperative Vulnerability Penetration Assessment Report

by Tim Honks, Wim Bonks, Julio Hernandez, Jebel Macias, Slick Will, Danny O'Boy

To update document, double-click then delete this line

|  |
| --- |
| Classified by:  Derived from: Guide 2  Declassify on: 11/02/2020 |

**DESTRUCTION NOTICE**

Destroy by any method that will prevent disclosure of contents or reconstruction of the document.

**DISCLAIMER**

The findings in this report are not to be construed as an official Department of the Army position unless so specified by other official documentation.

**WARNING**

Information and data contained in this document are based on the input available at the time of preparation.

**TRADE NAMES**

The use of trade names in this report does not constitute an official endorsement or approval of the use of such commercial hardware or software. The report may not be cited for purposes of advertisement.

**November 2020**



Combat Capabilities Development Command (CCDC) Data & Analysis Center (DAC) Cooperative Vulnerability Penetration Assessment Report

by Tim Honks, Wim Bonks, Julio Hernandez, Jebel Macias, Slick Will, Danny O'Boy

CCDC Data & Analysis Center

Author(s)

Affiliation

|  |
| --- |
| Classified by:  Derived from: Guide 2  Declassify on: 11/02/2020 |

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| REPORT DOCUMENTATION PAGE | | | | | | Form Approved | | |
| INTENTIONALLY LEFT BLANK | | | | | | | | |
| 1. REPORT DATE  November 2020 | | 2. REPORT TYPE  Cooperative Vulnerability Penetration Assessment | | | | 3. DATES COVERED *(From - To)*  01/2018 - 01/2019 | | |
| 4. TITLE AND SUBTITLE  Combat Capabilities Development Command (CCDC) Data & Analysis Center (DAC) Cooperative Vulnerability Penetration Assessment Report | | | | | | 5a. CONTRACT NUMBER | | |
| 5b. GRANT NUMBER | | |
| 5c. PROGRAM ELEMENT NUMBER | | |
| 6. AUTHOR(S)  Tim Honks, Wim Bonks, Julio Hernandez, Jebel Macias, Slick Will, Danny O'Boy | | | | | | 5d. PROJECT NUMBER | | |
| 5e. TASK NUMBER | | |
| 5f. WORK UNIT NUMBER | | |
| 7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)  Director  U.S. Army CCDC Data & Analysis Center  6896 Mauchly Street  Aberdeen Proving Ground, MD | | | | | | 8. PERFORMING ORGANIZATION REPORT  NUMBER | | |
|  | | |
| 9. SPONSORING / MONITORING AGENCY NAME(S) AND ADDRESS(ES) | | | | | | 10. SPONSOR/MONITOR’S ACRONYM(S) | | |
|  | | | | | |  | | |
|  | | |
| 11. SPONSOR/MONITOR’S REPORT | | |
| NUMBER(S) | | |
| 12. DISTRIBUTION / AVAILABILITY STATEMENT | | | | | | | | |
| 13. SUPPLEMENTARY NOTES | | | | | | | | |
| 14. ABSTRACT | | | | | | | | |
| 15. SUBJECT TERMS  Cooperative Vulnerability Penetration Assessment Report | | | | | | | | |
| 16. SECURITY CLASSIFICATION OF: | | | | 17. LIMITATION  OF ABSTRACT | 18. NUMBER OF PAGES | | 19a. NAME OF RESPONSIBLE PERSON  Name | |
| a. REPORT  UNCLASSIFIED | b. ABSTRACT  UNCLASSIFIED | | c. THIS PAGE  UNCLASSIFIED | SAME AS REPORT | 23 | | 19b. TELEPHONE NUMBER  *(include area code)*  Phone | |
|  | | | | | | | |  |

| Table of Contents |
| --- |
| [List of Figures iv](#_Toc38966248)  [List of Tables v](#_Toc38966249)  [Acknowledgements vi](#_Toc38966250)  [Executive Summary vii](#_Toc38966251)  [1. (U) Introduction 8](#_Toc38966252)  [1.1 (U) System/Network Architecture 9](#_Toc38966253)  [1.2 (U) Test Setup and Network Postures 10](#_Toc38966254)  [1.3 (U) Limitations 10](#_Toc38966255)  [2. Enter Event Type (e.g., CVPA, CVI, VoF, etc) Findings 11](#_Toc38966256)  [2.1 (U) Lack of Encryption 12](#_Toc38966257)  [2.2 (U) Missing Patches 14](#_Toc38966258)  [3. Conclusions and Recommendations 16](#_Toc38966259)  [Appendix A – List of Acronym A-1](#_Toc38966260)  [Appendix B – Distribution List B-1](#_Toc38966261) |

| List of Figures |
| --- |
| [Figure 1 Sample Caption 13](#_Toc38966262)  [Figure 2 Sample Caption 15](#_Toc38966263) |

| List of Tables |
| --- |
| Table 1. (S) List of Findings 11  Table 2 describes the Lack of Encryption vulnerability. 12  Table 3 describes the Missing Patches vulnerability. 14 |

###### Acknowledgements

The U.S. Army Combat Capabilities Development Command (CCDC) Data & Analysis Center (DAC) recognizes the following individuals for their contributions to this report:

The authors are

Tim Honks, Wim Bonks, Julio Hernandez, Jebel Macias, Slick Will, Danny O'Boy

The authors wish to acknowledge the contributions of the following individuals for his/her assistance in the creation of this report:

###### Executive Summary

# (U) Introduction

## (U) System/Network Architecture

The figure below provides an overview of the system/network architecture.

Describe the system architecture based on a high level diagram provided below.

<Insert a high level diagram of the system architecture>

## (U) Test Setup and Network Postures

## (U) Limitations

# Cooperative Vulnerability Penetration Assessment Findings

(U) Table 1 lists vulnerabilities identified and validated by CCDC DAC during the Cooperative Vulnerability Penetration Assessment with their associated technical risk.

**Table 1. (S) List of Findings**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **ID** | **DESCRIPTION** | **LIKELIHOOD** | **IMPACT** | **RISK** |
| **5fadac40a5270000df007ba7** | **This is a test description** | **VH** | **VH** | **M** |
| **5fadac40a5270000df007ba8** | **This is a test description** | **VH** | **VH** | **M** |
| **5fadac40a5270000df007ba9** | **This is a test description** | **VH** | **M** | **L** |
| **5fadac40a5270000df007baa** | **This is a test description** | **VH** | **M** | **L** |
| **5fadac40a5270000df007bab** | **This is a test description** | **VH** | **M** | **L** |
| **5fadac40a5270000df007bac** | **This is a test description** | **VH** | **M** | **L** |
| **5fadac40a5270000df007bad** | **This is a test description** | **VH** | **M** | **L** |
| **5fadac40a5270000df007bae** | **This is a test description** | **VH** | **M** | **L** |
| **5fadac40a5270000df007baf** | **This is a test description** | **VH** | **M** | **L** |
| **5fadac40a5270000df007bb0** | **This is a test description** | **VH** | **M** | **L** |

## (U) Finding 1

Table 1 describes the Finding 1 vulnerability.

**Table 1. Finding 1**

|  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **ID** | **5fadac40a5270000df007ba7** |  | **IMPACT SCORE** | 4 | **STATUS** | **Open** | **POSTURE** | | |
| **HOST NAMES** | | **IP:PORT** | **CAT** | I | **LIKELIHOOD** | **VH** | Nearsider | | |
| Host1 | | 127.19.12.2:80 | **CAT SCORE** | 4 | **IMPACT** | **VH** |
| **VS-SCORE** | 40.0 | **RISK** | **M** | **C** | **I** | **A** |
| **VS** | **M** | **CM** | VH | Y | Y | Y |
| **IMPACT RATIONALE** | This is a test impact description | | | | | |
| **TYPE** | | Creds | | | | | | | |
|  | Finding 1 | | | | | | | | |
| **DESCRIPTION** | This is a test description | | | | | | | | |
|  | Test | | | | | | | | |
| **MITIGATION** | This is a test long description | | | | | | | | |
| **REFERENCES** | | Figure 1 | | | | | | | |
| C-CONFIDENTIALITY I-INTEGRITY A-AVAILABILITY CM-COUNTERMEASURE | | | | | | | | | |

Information

Information

Information

Figure 1

## (U) Finding 2

Table 2 describes the Finding 2 vulnerability.

**Table 2. Finding 2**

|  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **ID** | **5fadac40a5270000df007ba8** |  | **IMPACT SCORE** | 4 | **STATUS** | **Closed** | **POSTURE** | | |
| **HOST NAMES** | | **IP:PORT** | **CAT** | II | **LIKELIHOOD** | **VH** | Outsider | | |
| Host2 | | 127.19.12.2:80 | **CAT SCORE** | 7 | **IMPACT** | **VH** |
| **VS-SCORE** | 40.0 | **RISK** | **M** | **C** | **I** | **A** |
| **VS** | **M** | **CM** | L | Y | Y | Y |
| **IMPACT RATIONALE** | This is a test impact description | | | | | |
| **TYPE** | | Creds | | | | | | | |
|  | Finding 2 | | | | | | | | |
| **DESCRIPTION** | This is a test description | | | | | | | | |
|  | Test | | | | | | | | |
| **MITIGATION** | This is a test long description | | | | | | | | |
| **REFERENCES** | | Figure 1 | | | | | | | |
| C-CONFIDENTIALITY I-INTEGRITY A-AVAILABILITY CM-COUNTERMEASURE | | | | | | | | | |

Information

Information

Information

Figure 1

## (U) Finding 3

Table 3 describes the Finding 3 vulnerability.

**Table 3. Finding 3**

|  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **ID** | **5fadac40a5270000df007ba9** |  | **IMPACT SCORE** | 4 | **STATUS** | **Open** | **POSTURE** | | |
| **HOST NAMES** | | **IP:PORT** | **CAT** | I | **LIKELIHOOD** | **VH** | Nearsider | | |
| Host3 | | 127.19.12.2:80 | **CAT SCORE** | 4 | **IMPACT** | **M** |
| **VS-SCORE** | 40.0 | **RISK** | **L** | **C** | **I** | **A** |
| **VS** | **M** | **CM** | VL | Y | Y | Y |
| **IMPACT RATIONALE** | This is a test impact description | | | | | |
| **TYPE** | | Creds | | | | | | | |
|  | Finding 3 | | | | | | | | |
| **DESCRIPTION** | This is a test description | | | | | | | | |
|  | Test | | | | | | | | |
| **MITIGATION** | This is a test long description | | | | | | | | |
| **REFERENCES** | | Figure 1 | | | | | | | |
| C-CONFIDENTIALITY I-INTEGRITY A-AVAILABILITY CM-COUNTERMEASURE | | | | | | | | | |

Information

Information

Information

Figure 1

## (U) Finding 4

Table 4 describes the Finding 4 vulnerability.

**Table 4. Finding 4**

|  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **ID** | **5fadac40a5270000df007baa** |  | **IMPACT SCORE** | 4 | **STATUS** | **Open** | **POSTURE** | | |
| **HOST NAMES** | | **IP:PORT** | **CAT** | I | **LIKELIHOOD** | **VH** | Nearsider | | |
| Host4 | | 127.19.12.2:80 | **CAT SCORE** | 4 | **IMPACT** | **M** |
| **VS-SCORE** | 40.0 | **RISK** | **L** | **C** | **I** | **A** |
| **VS** | **M** | **CM** | VL | Y | Y | Y |
| **IMPACT RATIONALE** | This is a test impact description | | | | | |
| **TYPE** | | Creds | | | | | | | |
|  | Finding 4 | | | | | | | | |
| **DESCRIPTION** | This is a test description | | | | | | | | |
|  | Test | | | | | | | | |
| **MITIGATION** | This is a test long description | | | | | | | | |
| **REFERENCES** | | Figure 1 | | | | | | | |
| C-CONFIDENTIALITY I-INTEGRITY A-AVAILABILITY CM-COUNTERMEASURE | | | | | | | | | |

Information

Information

Information

Figure 1

## (U) Finding 5

Table 5 describes the Finding 5 vulnerability.

**Table 5. Finding 5**

|  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **ID** | **5fadac40a5270000df007bab** |  | **IMPACT SCORE** | 4 | **STATUS** | **Open** | **POSTURE** | | |
| **HOST NAMES** | | **IP:PORT** | **CAT** | I | **LIKELIHOOD** | **VH** | Nearsider | | |
| Host4 | | 127.19.12.2:80 | **CAT SCORE** | 4 | **IMPACT** | **M** |
| **VS-SCORE** | 40.0 | **RISK** | **L** | **C** | **I** | **A** |
| **VS** | **M** | **CM** | VL | Y | Y | Y |
| **IMPACT RATIONALE** | This is a test impact description | | | | | |
| **TYPE** | | Creds | | | | | | | |
|  | Finding 5 | | | | | | | | |
| **DESCRIPTION** | This is a test description | | | | | | | | |
|  | Test | | | | | | | | |
| **MITIGATION** | This is a test long description | | | | | | | | |
| **REFERENCES** | | Figure 1 | | | | | | | |
| C-CONFIDENTIALITY I-INTEGRITY A-AVAILABILITY CM-COUNTERMEASURE | | | | | | | | | |

Information

Information

Information

Figure 1

## (U) Finding 6

Table 6 describes the Finding 6 vulnerability.

**Table 6. Finding 6**

|  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **ID** | **5fadac40a5270000df007bac** |  | **IMPACT SCORE** | 4 | **STATUS** | **Open** | **POSTURE** | | |
| **HOST NAMES** | | **IP:PORT** | **CAT** | I | **LIKELIHOOD** | **VH** | Nearsider | | |
| Host4 | | 127.19.12.2:80 | **CAT SCORE** | 4 | **IMPACT** | **M** |
| **VS-SCORE** | 40.0 | **RISK** | **L** | **C** | **I** | **A** |
| **VS** | **M** | **CM** | VL | Y | Y | Y |
| **IMPACT RATIONALE** | This is a test impact description | | | | | |
| **TYPE** | | Creds | | | | | | | |
|  | Finding 6 | | | | | | | | |
| **DESCRIPTION** | This is a test description | | | | | | | | |
|  | Test | | | | | | | | |
| **MITIGATION** | This is a test long description | | | | | | | | |
| **REFERENCES** | | Figure 1 | | | | | | | |
| C-CONFIDENTIALITY I-INTEGRITY A-AVAILABILITY CM-COUNTERMEASURE | | | | | | | | | |

Information

Information

Information

Figure 1

## (U) Finding 7

Table 7 describes the Finding 7 vulnerability.

**Table 7. Finding 7**

|  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **ID** | **5fadac40a5270000df007bad** |  | **IMPACT SCORE** | 4 | **STATUS** | **Open** | **POSTURE** | | |
| **HOST NAMES** | | **IP:PORT** | **CAT** | I | **LIKELIHOOD** | **VH** | Nearsider | | |
| Host4 | | 127.19.12.2:80 | **CAT SCORE** | 4 | **IMPACT** | **M** |
| **VS-SCORE** | 40.0 | **RISK** | **L** | **C** | **I** | **A** |
| **VS** | **M** | **CM** | VL | Y | Y | Y |
| **IMPACT RATIONALE** | This is a test impact description | | | | | |
| **TYPE** | | Creds | | | | | | | |
|  | Finding 7 | | | | | | | | |
| **DESCRIPTION** | This is a test description | | | | | | | | |
|  | Test | | | | | | | | |
| **MITIGATION** | This is a test long description | | | | | | | | |
| **REFERENCES** | | Figure 1 | | | | | | | |
| C-CONFIDENTIALITY I-INTEGRITY A-AVAILABILITY CM-COUNTERMEASURE | | | | | | | | | |

Information

Information

Information

Figure 1

## (U) Finding 8

Table 8 describes the Finding 8 vulnerability.

**Table 8. Finding 8**

|  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **ID** | **5fadac40a5270000df007bae** |  | **IMPACT SCORE** | 4 | **STATUS** | **Open** | **POSTURE** | | |
| **HOST NAMES** | | **IP:PORT** | **CAT** | I | **LIKELIHOOD** | **VH** | Nearsider | | |
| Host4 | | 127.19.12.2:80 | **CAT SCORE** | 4 | **IMPACT** | **M** |
| **VS-SCORE** | 40.0 | **RISK** | **L** | **C** | **I** | **A** |
| **VS** | **M** | **CM** | VL | Y | Y | Y |
| **IMPACT RATIONALE** | This is a test impact description | | | | | |
| **TYPE** | | Creds | | | | | | | |
|  | Finding 8 | | | | | | | | |
| **DESCRIPTION** | This is a test description | | | | | | | | |
|  | Test | | | | | | | | |
| **MITIGATION** | This is a test long description | | | | | | | | |
| **REFERENCES** | | Figure 1 | | | | | | | |
| C-CONFIDENTIALITY I-INTEGRITY A-AVAILABILITY CM-COUNTERMEASURE | | | | | | | | | |

Information

Information

Information

Figure 1

## (U) Finding 9

Table 9 describes the Finding 9 vulnerability.

**Table 9. Finding 9**

|  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **ID** | **5fadac40a5270000df007baf** |  | **IMPACT SCORE** | 4 | **STATUS** | **Open** | **POSTURE** | | |
| **HOST NAMES** | | **IP:PORT** | **CAT** | I | **LIKELIHOOD** | **VH** | Nearsider | | |
| Host4 | | 127.19.12.2:80 | **CAT SCORE** | 4 | **IMPACT** | **M** |
| **VS-SCORE** | 40.0 | **RISK** | **L** | **C** | **I** | **A** |
| **VS** | **M** | **CM** | VL | Y | Y | Y |
| **IMPACT RATIONALE** | This is a test impact description | | | | | |
| **TYPE** | | Creds | | | | | | | |
|  | Finding 9 | | | | | | | | |
| **DESCRIPTION** | This is a test description | | | | | | | | |
|  | Test | | | | | | | | |
| **MITIGATION** | This is a test long description | | | | | | | | |
| **REFERENCES** | | Figure 1 | | | | | | | |
| C-CONFIDENTIALITY I-INTEGRITY A-AVAILABILITY CM-COUNTERMEASURE | | | | | | | | | |

Information

Information

Information

Figure 1

## (U) Finding 10

Table 10 describes the Finding 10 vulnerability.

**Table 10. Finding 10**

|  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **ID** | **5fadac40a5270000df007bb0** |  | **IMPACT SCORE** | 4 | **STATUS** | **Open** | **POSTURE** | | |
| **HOST NAMES** | | **IP:PORT** | **CAT** | I | **LIKELIHOOD** | **VH** | Nearsider | | |
| Host4 | | 127.19.12.2:80 | **CAT SCORE** | 4 | **IMPACT** | **M** |
| **VS-SCORE** | 40.0 | **RISK** | **L** | **C** | **I** | **A** |
| **VS** | **M** | **CM** | VL | Y | Y | Y |
| **IMPACT RATIONALE** | This is a test impact description | | | | | |
| **TYPE** | | Creds | | | | | | | |
|  | Finding 10 | | | | | | | | |
| **DESCRIPTION** | This is a test description | | | | | | | | |
|  | Test | | | | | | | | |
| **MITIGATION** | This is a test long description | | | | | | | | |
| **REFERENCES** | | Figure 1 | | | | | | | |
| C-CONFIDENTIALITY I-INTEGRITY A-AVAILABILITY CM-COUNTERMEASURE | | | | | | | | | |

Information

Information

Information

Figure 1

# Conclusions and Recommendations

Insert conclusions write up here

1. – List of Acronym

|  |  |
| --- | --- |
|  |  |
| CCDC | Combat Capabilities Development Command |
|  |  |
| DAC | Data & Analysis Center |
|  |  |
|  |  |

1. – Distribution List

Organization