Baseline Security Requirements and Proof of Concept Design Document

# Team 1

Riley Dorough

Kayla Echols

Julia Wilkins

Brett Wolff

October 2nd, 2021

**Table of Contents**

|  |  |  |
| --- | --- | --- |
| **Section/Sub-section Title** | **Author** | **Page #** |
| **1. Introduction**  **1.1 OWASP Top 10 Findings**  **1.2 Code Review** | James Dorough | 2 |
| **2. Network**  **2.1 Topology**  **2.2 List of Services and Operating Systems** | James Dorough | 3 |
| **3. Host 1: Windows 10**  **3.1 CVE 1 and Mitigation**  **3.2 CVE 2 and Mitigation**  **3.3 CVE 3 and Mitigation**  **3.4 CVE 4 and Mitigation**  **3.5 CVE 5 and Mitigation** | Brett Wolff | 5 |
| **4. Host 2: Windows Server 2016**  **4.1 CVE 1 and Mitigation**  **4.2 CVE 2 and Mitigation**  **4.3 CVE 3 and Mitigation**  **4.4 CVE 4 and Mitigation**  **4.5 CVE 5 and Mitigation** | Julia Wilkins | 5 |
| **5. Host 3: Ubuntu**  **5.1 CVE 1 and mitigation**  **5.2 CVE 2 and mitigation**  **5.3 CVE 3 and mitigation**  **5.4 CVE 4 and mitigation**  **5.5 CVE 5 and mitigation** | Kayla Echols | 6 |
| **6. Host 4: PfSense**  **6.1 CVE 1 and mitigation**  **6.2 CVE 2 and mitigation**  **6.3 CVE 3 and mitigation** | Julia Wilkins | 7 |
| **7. Penetration Testing Findings**  **7.1 Summary Graphs**  **7.2 Action Items & Areas of Interest** |  | 8 |
| **8. End Matter**  **8.1 Acronyms**  **8.2 References**  **8.3 Appendices** | Julia Wilkins | 8 |

1. **Introduction**
   1. **OWASP Top 10 Findings**

Anticipated top ten risks to the project.

* + 1. Default Credentials
    2. Poor credential security practice
    3. Social Engineering
    4. Unencrypted Communications
    5. Critical information & PII leakage
    6. Host DOS/DDOS
    7. Web Directory Enumeration
    8. Public Page DOS/DDOS
    9. Man in the Middle attack MITM
    10. Windows Remote Desktop Protocol (RDP)
  1. **Code Review**

Nearly all tools used in this project are open source other than some OSs and proprietary software (Microsoft tools). The code team 1 develops will be using Microsoft’s .NET Framework and will be designed from the ground up with security in mind.

1. **Network**
   1. **Topology**

**Diagram

Description automatically generated with medium confidence**

* 1. **List of Services and Operating Systems**

|  |  |
| --- | --- |
| **Host/ Service** | **Details/ OS/ Service** |
| Host:  Windows 10 | Windows 10 Pro,  Version 21H1,  OS build: 19043.1237,  Current date of OS revision: 2021-09-14  Security Intel Version 1.349.1635.0  Security Intel date of revision: 2021-09-29 |
| Host:  Windows Server 2016 | Windows Server 2016 Standard,  Version 1607,  Current date of OS revision: 2021-09-14 |
| Service:  OpenHistorian | Version 20.8.45.0,  Database type: MySQL Version 8.0.26 |
| Host:  Ubuntu Desktop | Ubuntu Desktop 20.04,  Version 20.04.3 LTS,  Current date of last OS revision 2021-08-19 |
| Service:  Docker | Version 20.10.7  API Version: 1.41  Current date of last software revision 2021-08-04 |
| Service:  pfSense | Version 2.4.5-RELEASE-p1  Current date of last software revision 2020-06-02 |

1. **Host 1: Windows 10**

|  |  |  |
| --- | --- | --- |
| **CVE ID** | **Description (versions effected and vulnerability details)** | **Mitigation Strategy** |
| CVE-2021-34527 | A remote code execution vulnerability exists when the Windows Print Spooler service improperly performs privileged file operations. An attacker who successfully exploited this vulnerability could run arbitrary code with SYSTEM privileges. An attacker could then install programs; view, change, or delete data; or create new accounts with full user rights. | There are vendor solutions available as well as registry settings that can be changed to a value of zero or undefined to prevent exploitation and remote code execution. |
| CVE-2021-34448 (787) | Scripting Engine Memory Corruption Vulnerability affecting 21H1 systems. | Install the patch for the vulnerability. |
| CVE-2021-36965 | Windows WLAN AutoConfig Service Remote Code Execution Vulnerability | Ensure correct patch is installed on system |
| CVE-2021-31956 | Windows NTFS Elevation of Privilege Vulnerability. To exploit this vulnerability, an attacker would first have to log on to the system. An attacker could then run a specially crafted application that could exploit the vulnerability and take control of an affected system.  Additionally, an attacker could convince a local user to open a malicious file. The attacker would have to convince the user to click a link, typically by way of an enticement in an email or instant message, and then convince them to open the specially crafted file. | Install the patch for the vulnerability. |
| CVE-2021-38634 | Microsoft Windows Update Client Elevation of Privilege Vulnerability. The specific flaw exists within Windows Update Agent. By creating a directory junction, an attacker can abuse Windows Update Agent to delete a file. An attacker can leverage this vulnerability to escalate privileges and execute arbitrary code in the context of SYSTEM. | Ensure correct patch is installed on system |

1. **Host 2: Windows Server 2016**

|  |  |  |
| --- | --- | --- |
| **CVE ID** | **Description (versions effected and vulnerability details)** | **Mitigation Strategy** |
| CVE-2021-40447 | Windows Print Spooler Elevation of Privilege Vulnerability | Ensure that Windows Sever remains updated |
| CVE-2021-040444 | Microsoft MSHTML Remote Code Execution Vulnerability | Open documents from the internet in protected view or use Application Guard for Office |
| CVE-2021-38638 | Windows Ancillary Function Driver for WinSock Elevation of Privilege Vulnerability | Ensure that Windows Server remains updated |
| CVE-2021-38637 | Windows Storage Information Disclosure Vulnerability | Ensure that Windows Server remains updated |
| CVE-2021-38636 | Windows Redirected Drive Buffering SubSystem Driver Information Disclosure Vulnerability | Ensure that Windows Server remains updated |

1. **Host 3: Ubuntu 20.04**

|  |  |  |
| --- | --- | --- |
| **CVE ID** | **Description (versions effected and vulnerability details)** | **Mitigation Strategy** |
| CVE-2021-33909 | The fs/seq\_file.c does not restrict seq buffer allocations, leading into integer overflow, an Out-of-bounds Write and escalation to root by an unprivileged use. | Install the latest version of Ubuntu or mitigate using host scanning. |
| CVE-2021-33910 | Basic unit-name.c in systemd memory allocation with excessive size value resulting in system crash. | **There is no mitigation at this time.** |
| CVE-2021-22555 | A heap out of bounds write affecting Linux since v.2.6.19-rc1 was discovered in net/netfilter/x\_tables.c. This allows an attacker to gain privileges or cause a DoS through username space. | Disable for unprivileged user possibilities of running unshare that can be done with the following command echo 0 > proc/sys/user/max\_user\_namespaces. |
| CVE-2021-3600 | It was discovered that the eBPF implementation in the Linux kernel did not properly track bounds information for 32 bit registers when preforming div and mod operations. A local attacker could use this to possibly execute arbitrary code. | A kernel update would be required to mitigate the flaw for the root or users with CAP\_SYS\_ADMIN capabilities. |
| CVE-2020-30465 | runc before 1.0.0-rc95 allows a Container Filesystem Breakout via Directory Traversal. To exploit the vulnerability, an attacker must be able to create multiple containers with a fairly specific mount configuration. The problem occurs via a symlink-exchange attack that relies on a race condition. | The impact of the vulnerability is reduced if SELinux is in enforcing mode using the container-selinux policy. |

1. **Host 4: PfSense**

|  |  |  |
| --- | --- | --- |
| **CVE ID** | **Description (versions effected and vulnerability details)** | **Mitigation Strategy** |
| CVE-2021-27933 | pfSense 2.5.0 allows XSS via the services\_wol\_edit.php Description field | Make sure PfSense is upgraded to 2.5.1 |
| CVE-2020-26693 | A stored cross-site scripting (XSS) vulnerability was discovered in pfSense 2.4.5-p1 which allows an authenticated attacker to execute arbitrary web scripts via exploitation of the load\_balancer\_monitor.php function. | Utilize corrections from GitHub |
| CVE-2020-19203 | An authenticated Cross-Site Scripting (XSS) vulnerability was found in widgets/widgets/wake\_on\_lan\_widget.php, a component of the pfSense software WebGUI, on version 2.4.4-p2 and earlier. The widget did not encode the descr (description) parameter of wake-on-LAN entries in its output, leading to a possible stored XSS. | Ensure latest version is utilized as well as any associated git hub corrections |

1. **Penetration Testing Findings**
   1. **Summary Graphs**

This section is not applicable currently. Summary of finding to follow once testing beings

* 1. **Action Items & Areas of Interest**

This Section is not currently applicable as Team 1 has not begun the testing phase.

1. **End Matter**
   1. **Acronyms**

None at this time

* 1. **References**

*Current CVSS score distribution for all vulnerabilities*. CVE security vulnerability database. Security vulnerabilities, exploits, references and more. (n.d.). Retrieved October 1, 2021, from https://www.cvedetails.com/.

*CVE Search r*. CVE. (n.d.). Retrieved October 1, 2021, from https://cve.mitre.org/cgi-bin/cvekey.cgi?keyword=CVE-2021-33909.

Microsoft. (n.d.). *MSRC researcher portal*. MSRC Researcher Portal. Retrieved October 1, 2021, from https://msrc.microsoft.com/.

NIST. (n.d.). *You are viewing this page in an unauthorized frame window.* National Vulnerability Database. Retrieved October 1, 2021, from https://nvd.nist.gov/.

Pfsense. (4841, January 1). *Fix encoding and validation on load\_balancer\_monitor\*. fixes #10940 · pfsense/PFSENSE@A220A22*. GitHub. Retrieved October 1, 2021, from https://github.com/pfsense/pfsense/commit/a220a22a8c05c10a7b875ac6b565f2c4fe7b251c.

*Red Hat CVE*. Red Hat Customer Portal - Access to 24x7 support and knowledge. (n.d.). Retrieved October 1, 2021, from https://access.redhat.com/security/cve/cve-2021-22555.

Ubuntu. (n.d.). *CVE search results*. Ubuntu CVE. Retrieved October 1, 2021, from https://ubuntu.com/security/cve?q=&package=&priority=high&version=focal&status=.

* 1. **Appendices**None at this time