Product: Shub

Report: Crazy Report

PEN-DOC20240115144454

Shub, https//:www.shub_pentest.com

15-01-2024

Project Overview

Description

fdsfs

Executive Summary

tbc

Summary of Findings Identified

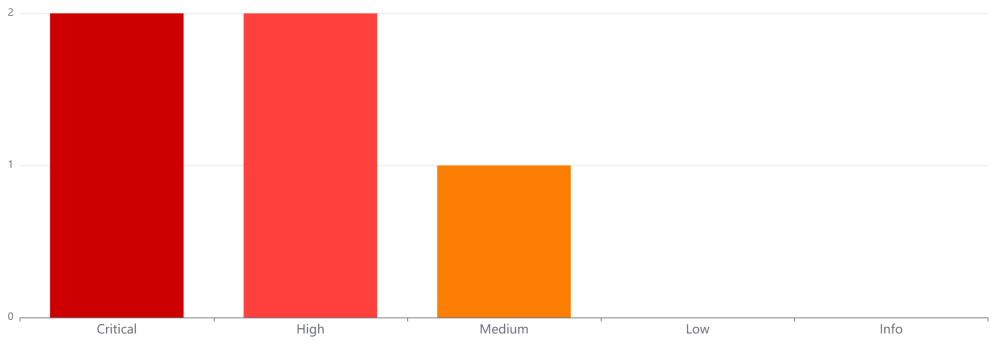

Figure 1: Executive Summary

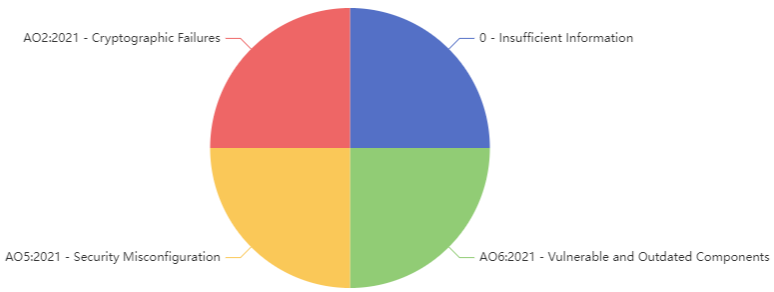

Figure 2: Breakdown by OWASP Categories

 # 1 High Operating System (OS) End of Life (EOL) Detection

 # 2 Critical BLOOP

 # 3 Critical Finding Test

 # 4 High Security MisConfig

 # 5 Medium MD5

Scope

In Scope

tbc

Out of Scope

tbc

Methodology

tbc

Recommendations

tbc

Findings and Risk Analysis

Operating System (OS) End of Life (EOL) Detection

Severity: High
CVSS Score: 10.0
CVSS Vector:

Description

The Operating System (OS) on the remote host has reached the end of life (EOL) and should not be used anymore.

Location

10.10.124.125

Impact

An EOL version of an OS is not receiving any security updates from the vendor. Unfixed security vulnerabilities might be leveraged by an attacker to compromise the security of this host.

Proof of Concept

The "Debian GNU/Linux" Operating System on the remote host has reached the end of life.

CPE: cpe:/o:debian:debian_linux:9 Installed version, build or SP: 9 EOL date: 2022-06-30 EOL info: https://en.wikipedia.org/wiki/List_of_Debian_releases#Release_table

Recommendation

Upgrade the OS on the remote host to a version which is still supported and receiving security updates by the vendor.

BLOOP

Severity: Critical
CVSS Score: 9.2
CVSS Vector: CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:N/VC:N/VI:H/VA:L/SC:N/SI:H/SA:N

OWASP

0 - Insufficient Information

Description

TBC

Impact

TBC

Recommendation

TBC

References

TBC

Finding Test

Severity: Critical
CVSS Score: 8.8
CVSS Vector: rewtgergerg

CWE

64 - Windows Shortcut Following (.LNK)

OWASP

6 - Vulnerable and Outdated Components

Description

Test

Location

Tbc

Impact

Tbc

Proof of Concept

Tbc

Recommendation

Tbc

References

Tbc

Security MisConfig

Severity: High
CVSS Score: 7.7
CVSS Vector: CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:N/VC:N/VI:N/VA:N/SC:N/SI:N/SA:H

OWASP

5 - Security Misconfiguration

Description

During the penetration test, a security misconfiguration vulnerability was identified. The server was exposing unnecessary and sensitive information to public networks. Issues identified included unneeded HTTP methods, verbose error messages providing too much information, and unpatched vulnerabilities in the server itself. These flaws make valuable targets and provide an attacker the opportunity for further exploits.

Location

https://example.com/admin

Impact

An attacker could take advantage of these misconfigurations to view sensitive data or unauthorized content, impacting the confidentiality, integrity, and availability of the system. This might allow for further compromise of the system, for example through issues such as server version disclosure leading to attack vector identification.

Proof of Concept

TBC

Recommendation

- Update and patch the software, infrastructure services, and custom-built applications.
- Remove unnecessary HTTP methods.
- Disable detailed error messages that could expose sensitive system or server information. Instead, opt for custom error pages.
- Regularly conduct vulnerability scans and assessments.
- Leverage the concept of least privilege at every layer of the application infrastructure.

References

- https://owasp.org/www-project-top-ten/OWASP_Top_Ten_2017/Top_10-2017_A6-Security_Misconfiguration
- https://cwe.mitre.org/data/definitions/16.html

Additional notes

Test Appendix

MD5

Severity: Medium
CVSS Score: 6.9
CVSS Vector: CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:N/VC:N/VI:N/VA:N/SC:L/SI:L/SA:N

OWASP

2 - Cryptographic Failures

Description

During the penetration testing, a high-severity vulnerability was discovered, classified as an OWASP A02:2021 - Cryptographic Failure. This vulnerability pertains to the inappropriate implementation or absence of encryption and hashing mechanisms to safeguard sensitive data. This can expose data to potential attackers, leading to potential unauthorized access and data breaches.

Location

https://example.com/admin

Impact

Apart from the direct risk of unauthorized access to sensitive data, this could also lead to a number of indirect consequences including legal implications, reputational damage and financial loss. More importantly, it may result in a loss of trust from customers and partners, as well as potential regulatory fines for non-compliance with data protection laws.

Proof of Concept

TBC

Recommendation

- Require developers to have basic understanding of cryptographic protocols and secure use of cryptography.
- Use strong, vetted cryptographic libraries with good security profiles and keep these libraries up to date with security patches.
- Verify effective use of encryption and hashing algorithms as per industry best practices.
- Consider implementing key management solutions to manage encryption keys effectively.
- Conduct regular security audits and penetration tests to detect vulnerabilities in a timely manner.

References

- http://cwe.mitre.org/data/definitions/327.html
- https://owasp.org/Top10/A02_2021-Cryptographic_Failures/
- https://www.owasp.org/index.php/Testing_for_Weak_Cryptography

Additional notes

Test Appendix Bloop bloop

NMap Scan Data

Additional Notes

Test Appendix

Wow what a crazy finding

Test Appendix

Wow what a crazy finding

Bloop bloop

MD5 is TRASHHHH