



VULNERABILITY ASSESMENT

SOJOSPECT

v1.0.0

Scanned by: admin

08/08/2023

GREEN FOSSIL PTE LTD



Table of Contents

1. Executive Summary.....2

2. Scan Results2

3. Our Findings.....2

4. Risk Assessment.....2

 Critical Severity Vulnerability.....2

 High Severity Vulnerability.....3

 Medium Severity Vulnerability3

 Low Severity Vulnerability3

5. Recommendations.....3

 Remediation.....4

1. Executive Summary

The purpose of this vulnerability scan is to gather data on Windows and third-party software patch levels on hosts in the SAMPLE-INC domain in the 00.00.00.0/01 subnet. Of the 300 hosts identified by SAMPLE-INC, 100 systems were found to be active and were scanned.

2. Scan Results

The raw scan results will be provided upon delivery.

3. Our Findings

The results from the credentialed patch audit are listed below. It is important to note that not all identified hosts were able to be scanned during this assessment – of the 300 hosts identified as belonging to the SAMPLE-INC domain, only 100 were successfully scanned. In addition, some of the hosts that were successfully scanned were not included in the host list provided.

OWASP Top 10 Checklist

| Severity | Vulnerability Type | Checked at |
|----------|-------------------------------------|---------------------|
| High | Injection | 2023-10-20 00:00:00 |
| High | SQL Injection | 2023-09-02 12:00:00 |
| Medium | Cross-Site Scripting (XSS) | 2023-09-02 12:00:00 |
| Low | Insecure Direct Object References | 2023-09-02 12:00:00 |
| High | Cross-Site Request Forgery (CSRF) | 2023-08-02 12:00:00 |
| Medium | Security Misconfiguration | 2023-08-02 12:00:00 |
| Medium | Sensitive Data Exposure | 2023-08-02 12:00:00 |
| Low | Broken Authentication | 2023-10-02 12:00:00 |
| High | XML External Entity Injection (XXE) | 2023-10-02 12:00:00 |
| Medium | Insecure Deserialization | 2023-10-02 12:00:00 |
| Low | Unvalidated Redirects and Forwards | 2023-10-02 12:00:00 |
| Low | Clickjacking | 2023-08-02 12:00:00 |
| High | Remote Code Execution (RCE) | 2023-08-02 12:00:00 |
| Medium | Server-Side Request Forgery (SSRF) | 2023-08-02 12:00:00 |
| Low | File Inclusion Vulnerabilities | 2023-08-02 12:00:00 |
| High | Insecure File Upload | 2023-08-02 12:00:00 |

4. Risk Assessment

This report identifies security risks that could have significant impact on mission-critical applications used for day-to-day business operations.

| | | | |
|-------------------|---------------|-----------------|--------------|
| Critical Severity | High Severity | Medium Severity | Low Severity |
| 286 | 171 | 116 | 0 |

High Severity Vulnerability

171 were unique high severity vulnerabilities. High severity vulnerabilities are often harder to exploit and may not provide the same access to affected systems.

A table of the top high severity vulnerabilities is provided below:

| Vulnerability | Description | Solution |
|---------------|-------------|----------|
|---------------|-------------|----------|

Medium Severity Vulnerability

116 were unique medium severity vulnerabilities. These vulnerabilities often provide information to attackers that may assist them in mounting subsequent attacks on your network. These should also be fixed in a timely manner but are not as urgent as the other vulnerabilities.

A table of the top high severity vulnerabilities is provided below:

| Vulnerability | Description | Solution |
|---------------|-------------|----------|
|---------------|-------------|----------|

Low Severity Vulnerability

No low severity vulnerabilities were found during this scan.

| Vulnerability | Description | Solution |
|---------------|-------------|----------|
| 222 | 22222 | 222222 |

5. Recommendations

Recommendations in this report are based on the available findings from the credentialed patch audit. Vulnerability scanning is only one tool to assess the security posture of a network. The results should not be interpreted as definitive measurement of the security posture of the SAMPLE-INC network. Other elements used to assess the current security posture would include policy review, a review of internal security controls and procedures, or internal red teaming/penetration testing.

Remediation

Taking the following actions across all hosts will resolve 96% of the vulnerabilities on the network:

| Action to Take | Description |
|----------------|-------------|
|----------------|-------------|

Additional Resources

External sources are listed below which can help fix issues:



TALK TO US

(65) 67751133

contactus@sp.edu.sg