VULNERABILITY ASSESMENT

SOJOSPECT

GREEN FOSSIL PTE LTD

SOJOSPECT Vulnerability Report

Table of Contents

Severity	Vulnerability Type	URL	Checked at
High	SQL Injection	https://chmsdemo.greenfossil...	2023-07-15 00:00:00
Medium	Cross-Site Scripting	https://chmsdemo.greenfossil...	2023-07-15 00:00:00

Low	Remote Code Execution	https://chmsdemo.greenfossil...	2023-07-15 00:00:00
Low	Authentication Bypass	https://chmsdemo.greenfossil...	2023-07-15 00:00:00
High	Insecure Direct Object References	https://chmsdemo.greenfossil...	2023-07-14 00:00:00
Medium	Cross-Site Request Forgery	https://chmsdemo.greenfossil...	2023-07-14 00:00:00
Low	Security Misconfiguration	https://chmsdemo.greenfossil...	2023-07-14 00:00:00
Low	Privilege Escalation	https://chmsdemo.greenfossil...	2023-07-14 00:00:00
High	Sensitive Data Exposure	https://chmsdemo.greenfossil...	2023-07-13 00:00:00
Medium	Brute Force Attacks	https://chmsdemo.greenfossil...	2023-07-13 00:00:00
Low	Weak Passwords	https://chmsdemo.greenfossil...	2023-07-13 00:00:00
Low	Information Disclosure	https://chmsdemo.greenfossil...	2023-07-13 00:00:00

User that ran the scan: U0000028
Time Scanned: 2023-07-18 23-47-24

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

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

Critical Severity Vulnerability

286 were unique critical severity vulnerabilities. Critical vulnerabilities require immediate attention. They are relatively easy for attackers to exploit and may provide them with full control of the affected systems.

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

PLUGIN NAME	DESCRIPTION	SOLUTION	COUNT
Mozilla Firefox < 65.0	The version of Firefox installed on the remote Windows host is prior to 65.0. It is therefore affected by multiple vulnerabilities as referenced in the mfsa2019-01 advisory.	Upgrade to Mozilla Firefox version 65.0 or later.	22
Mozilla Foundation Unsupported Application Detection	According to its version there is at least one unsupported Mozilla application (Firefox| Thunderbird| and/or SeaMonkey) installed on the remote host. This version of the software is no longer actively maintained.	Upgrade to a version that is currently supported.	16

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:

PLUGIN NAME	DESCRIPTION	SOLUTION	COUNT
MS15-124: Cumulative Security Update for Internet Explorer (3116180)	The version of Internet Explorer installed on the remote host is missing Cumulative Security Update 3116180. It is therefore affected by multiple vulnerabilities the majority of which are remote code execution vulnerabilities.	Microsoft has released a set of patches for Windows Vista, 2008, 7, 2008 R2, 8, RT 2012, 8.1, RT 8.1, 2012 R2, and 10.	24
Mozilla Firefox < 64.0 Multiple Vulnerabilities	The version of Mozilla Firefox installed on the remote Windows host is prior to 64.0. It is therefore affected by multiple vulnerabilities as noted in Mozilla Firefox stable channel update release notes for 2018/12/11.	Upgrade to Mozilla Firefox version 64.0 or later.	22

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:

PLUGIN NAME	DESCRIPTION	SOLUTION	COUNT
Mozilla Firefox < 62.0.2 Vulnerability	The version of Mozilla Firefox installed on the remote Windows host is prior to 62.0.2. It is therefore affected by a vulnerability as noted in Mozilla Firefox stable channel update release notes for 2018/09/21.	Upgrade to Mozilla Firefox version 62.0.2 or later.	17
Mozilla Firefox < 57.0.4 Speculative Execution Side-Channel Attack Vulnerability (Spectre)	The version of Mozilla Firefox installed on the remote Windows host is prior to 57.0.4. It is therefore vulnerable to a speculative execution side-channel attack. Code from a malicious web page could read data from other web sites or private data from the browser itself.	Upgrade to Mozilla Firefox version 57.0.4 or later.	15

Low Severity Vulnerability

No low severity vulnerabilities were found during this scan.

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	VULNS	HOSTS
Lorem ipsum dolor sit amet, consectetur adipiscing elit. In a semper felis.	82	3
Integer finibus et erat et viverra. Cras at bibendum nisi. Pellentesque magna nisi, dictum ac augue quis, pulvinar ullamcorper ex.	16	10
Sed ac mattis odio, et pharetra ex. Etiam vitae scelerisque ipsum.	7	6
Fusce in arcu eget velit auctor venenatis. Ut sagittis ipsum neque, a tincidunt leo imperdiet maximus.Nulla ac sodales ipsum.	8	3

Additional Resources

External sources are listed below which can help fix issues:

OWASP Top Ten

TALK TO US

(04) 298 3985 2092
+76 209 1092 4095
info@mollysrestaurant.com