NETIZEN®
CyberSecure Solutions

External Evaluation Sample

July 29, 2020

PREPARED EXCLUSIVELY FOR:

Sample Co.

NOTICE:

This document contains sensitive and confidential information regarding the information security at Sample Co.. Appropriate care should be taken to secure this document from unauthorized access.

TABLE OF CONTENTS

1.0 EXECUTIVE SUMMARY

1.1 Introduction

Netizen Corporation was contracted by Sample Co. to conduct an external vulnerability evaluation in order to determine its current exposure level to a targeted attack. The vulnerability assessment was conducted in a manner that simulated a malicious actor engaged in a targeted attack against Sample Co. with the goal(s) of:

- Locating and identifying current information system vulnerabilities on external networks belonging to Sample Co.

All efforts were placed on the identification of security weaknesses that could allow a remote and/or internal attacker to compromise the confidentiality, integrity, and availability of the information systems. The scans were conducted with the level of access that a general external and/or internal user would have.

1.2 Scope of Work

Vulnerability scanning was performed on both external and internal IPs provided by Sample Co.:

Network Address:

- https://snydersvilleraceway.com
- https://orevillekartclub.org
- 18.209.154.54

Every IP endpoint was scanned for services running on all IANA assigned TCP ports. Any services that were deemed running received further vulnerability testing. The vulnerability scan was set below a threshold that would not impact a production environment, but it still allowed for enough depth to find significant security vulnerabilities.

The vulnerability scan results are compiled together and rated based on their risk factor, which is outlined below:

Critical	Verified vulnerability that was exploited for access
High	Poses a significant risk and is probably an avenue of attack
Medium	May pose a risk, but it is not directly exploitable
Low	Informational, and/or extremely unlikely to be a risk

The goal of the external evaluation is to view the current state of the network based on a database of know exploits and vulnerabilities. This will help in determining the overall security posture of Sample Co..

1.3 Summary of Results

During the external assessment, three medium vulnerabilities were discovered consisting of Apache Struts Directory Traversal exploits and expired SSL/TLS Certificates. Approximately 2 web addresses and 1 IP address were scanned during the evaluation. No other notable discoveries were found externally.

1.4 Summary of Recommendations

Regarding the external vulnerability results, the use of weak SSL/TLS certificates and protocols should be addressed to ensure that no sensitive data is exploited. This weakness could potentially allow malicious actors to further compromise the services or devices that are exposed. Mitigation efforts typically include configuration changes or applicable vendor updates.

Most organizations lack the in-house security expertise to ensure adequate levels of protection and compliance on an ongoing basis. Because of this, a once protected organization may regress into becoming vulnerable. As such, we recommend network and application scanning services combined with our proprietary dashboard, the Overwatch Governance Suite ™ (OGS) that would alert your company. users to critical issues and vulnerabilities so that they can be remediated in a timely manner. The OGS helps to ensure that your company isn't just secure in this one' snapshot' in time, but that your company continues to have visibility into their security stance on a daily basis for the coming year.

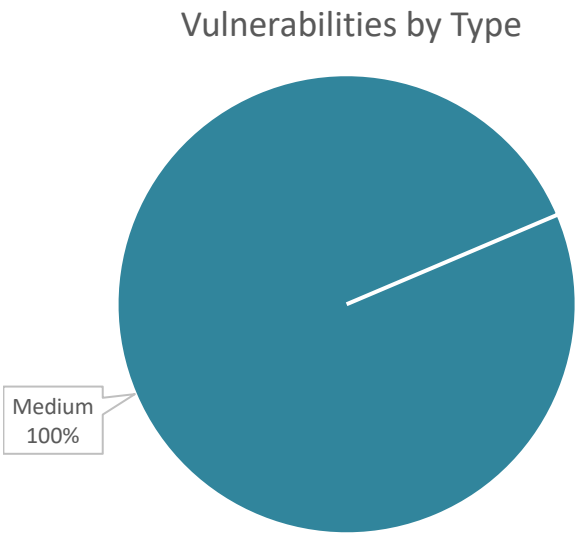
Vulnerability monitoring can help an enterprise's IT staff identify weaknesses throughout its network, such as ports that could be accessed by unauthorized users, misconfigurations, default or easy to guess passwords and software lacking the latest security patches, helping to ensure network compliance with the organization's security policy. This can be pursued in one of two different methods.

The first is "passive" monitoring. This is an uncredentialed scan in which the designated IP ranges are scanned and the results posted to the OGS that is accessible 24x7 to you or your Managed Services Provider (MSP). You or Your managed security provider will then check the OGS for new findings and complete and remediation actions as required. The scan frequency is as desired by our clients, from nightly to once per week or other schedules.

"Active" monitoring is a credentialed (internal only) or uncredentialed scan of the designated IP ranges. Like the passive scan, the results are uploaded to the OGS and are always accessible. The advantage being our SOC engineers will monitor the results of the scans and report any issues as desired by your company. The SOC engineers will also participate in calls with you or your Managed Services Provider when desired to assist in the triage of determining criticality and remediation suggestions. This would also include a rescan/ checking of the next scheduled scan to ensure items are indeed remediated.

2.0 EXTERNAL EVALUATION RESULTS

2.1 *Initial Results / Recon Overview*



0	0	2	0

2.2 Apache Struts Directory Traversal Vulnerability (S2-004)

MEDIUM VULNERABILITY

DESCRIPTION

This host is running Apache Struts and is prone to Directory Traversal Vulnerability.

Input validation error within the user supplied request URI while read arbitrary files via '../' with a '/struts/' path which is related to FilterDispatcher and DefaultStaticContentLoader.

ATTACK SCENARIO

Successful exploitation will let the attacker launch directory traversal attack and gain sensitive information about the remote system directory contents.

RECOMMENDATION

Upgrade to a minimum of Struts 2.0.12 or 2.1.6.

TAGS

CVSS:5.0

AFFECTED ASSETS

1. 18.209.154.54

NOTES

URL:http://secunia.com/advisories/32497, URL:https://cwiki.apache.org/confluence/display/WW/S2-004, URL:http://issues.apache.org/struts/browse/WW-2779

STEPS TO REPRODUCE

Vulnerable URL: https://orevillekartclub.org/struts/struts/..%252f..%252f..%252fWEB-INF

2. 18.209.154.54

NOTES

URL:http://secunia.com/advisories/32497, URL:https://cwiki.apache.org/confluence/display/WW/S2-004, URL:http://issues.apache.org/struts/browse/WW-2779

STEPS TO REPRODUCE

Vulnerable URL: https://snydersvilleraceway.com/struts/struts/..%252f..%252f..%252fWEB-INF

2.3 SSL/TLS: Certificate In Chain Expired

MEDIUM VULNERABILITY

DESCRIPTION
The remote service is using a SSL/TLS certificate chain where one or multiple CA certificates have expired.

The script checks if the CA certificates in the SSL/TLS certificate chain have expired.

ATTACK SCENARIO
N/A

RECOMMENDATION
Sign your server certificate with a valid CA certificate.

TAGS
CVSS:5.0

AFFECTED ASSETS
1. 18.209.154.54

STEPS TO REPRODUCE
The following certificates which are part of the certificate chain have expired: Subject: CN=AddTrust External CA Root,OU=AddTrust External TTP Network,O=AddTrust AB,C=SE Expired on: 2020-05-30 10:48:38 Subject: CN=USERTrust RSA Certification Authority,O=The USERTRUST Network,L=Jersey City,ST=New Jersey,C=US Expired on: 2020-05-30 10:48:38

3.0 APPENDIX B: Overview Explained

Total Vulnerabilities	Summary of unique vulnerabilities that were identified during this engagement against the items within scope. A unique vulnerability is a single vulnerability that may have multiple instances i.e. multiple targets / assets in scope who are affected by the same vulnerability will be considered as one unique vulnerability.
Zero-Day Vulnerability	A zero-day vulnerability is a vulnerability in software that is unknown to the vendor or developer and to your organisation. This security hole is often exploited by hackers before the vendor, developer or your organisation becomes aware and hurries to fix it. A zero-day attack can include infiltrating malware, spyware, or allowing unwanted access to sensitive or confidential information.
Easily Exploitable Vulnerability	Easily exploitable vulnerabilities are weaknesses that are often easy to detect typically through use of automated tools and scanners, have public exploits available, and/or can be exploited by an adversary with little required effort & skill.
Critical Priority Vulnerability	Vulnerabilities in this category can lead to significant impact on confidentiality, integrity and/or availability of organisational systems and data if not addressed immediately.
High Priority Vulnerability	Vulnerabilities in this category require immediate attention and plan for action.
Medium Priority Vulnerability	Vulnerabilities in this category are less urgent however in some circumstances may still pose a serious threat or consequence.
Low Priority Vulnerability	Vulnerabilities in this category are not an imminent threat however should be addressed to avoid issues in the longer term.

4.0 APPENDIX C: Severity Definitions

Severity	Description
CRITICAL Likelihood to be exploited: Within next 12 months	- The event is expected to occur in most circumstances - Definite probability - Has happened in the past and nil compensating controls have been implemented - Unavoidable – it will happen - Without additional controls the event is expected to occur in most circumstances
HIGH Likelihood to be exploited: 50% chance within next 12 months	- The event will probably occur in most circumstances - With existing controls in place this event will probably occur with some certainty - Events like this has occurred regularly in the industry
MEDIUM Likelihood to be exploited: 10% chance within next 12 months	- The event should occur in some circumstances - The event has occurred in different industries
LOW Likelihood to be exploited: 1% chance within next 12 months	- The event could occur in some circumstances - The event hasn't occurred in the business, it could occur in some circumstances