YourIT!
Your Logo Goes Here

PCI Assessment

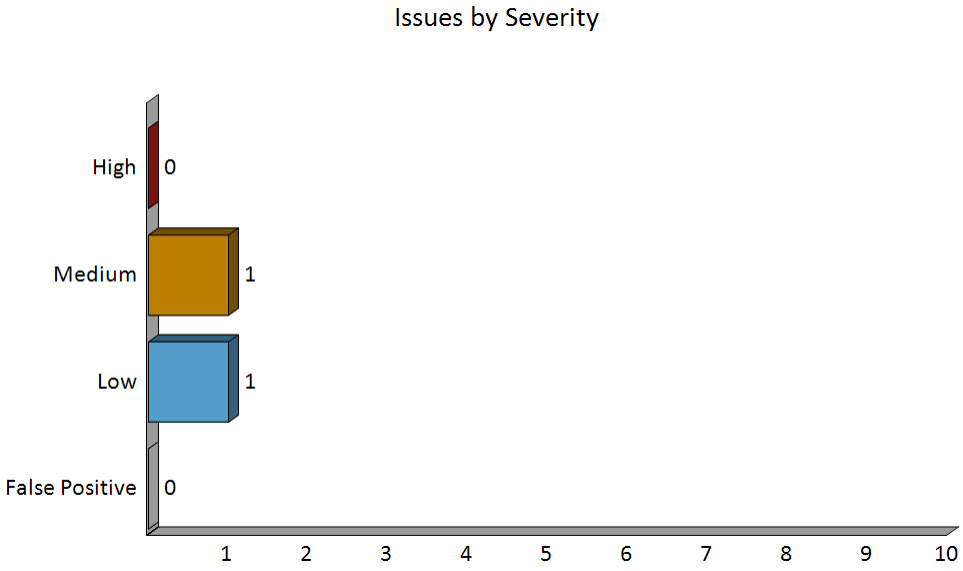
External Vulnerability Scan Detail by Issue Report

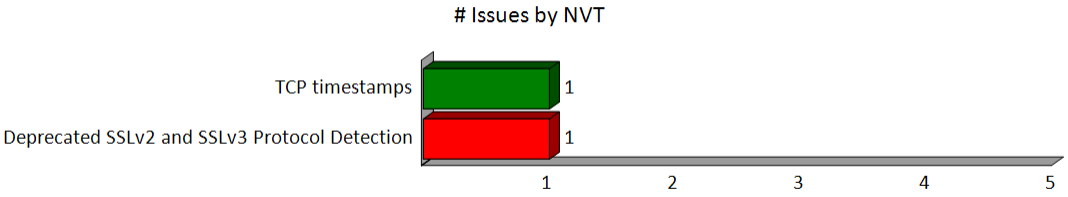
Prepared for:
Prospect Or Customer
Prepared by:
Your Company Name

Table of Contents

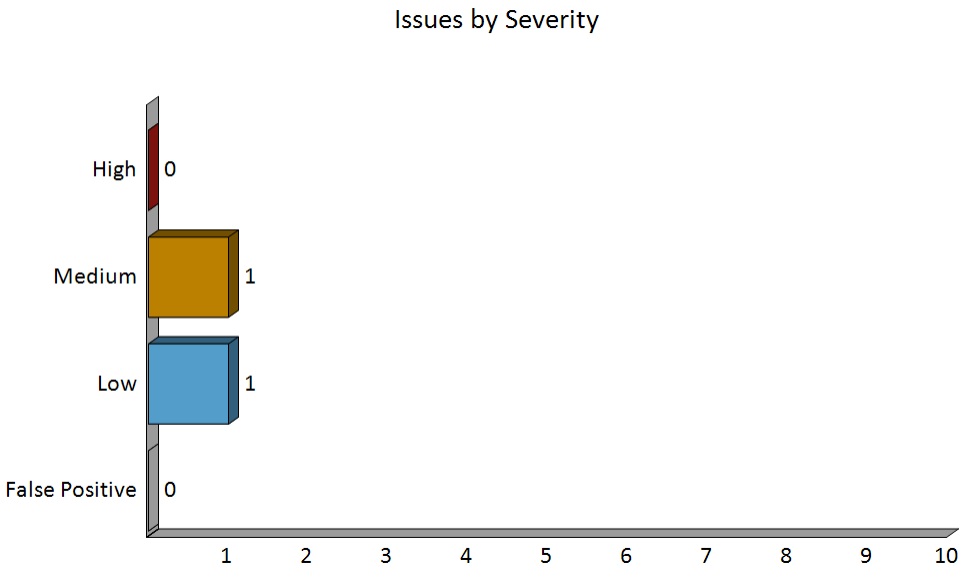
1 - Summary

This report gives details on hosts that were tested and issues that were found group by individual issues.





2 - Scan Details



2.1 - Deprecated SSLv2 and SSLv3 Protocol Detection

Medium (CVSS: 4.3) OID: 1.3.6.1.4.1.25623.1.0.111012	443/tcp (https)
Summary It was possible to detect the usage of the deprecated SSLv2 and/or SSLv3 protocol on this system.	
Affected Nodes 199.38.223.84	
Vulnerability Detection Result In addition to TLSv1+ the service is also providing the deprecated SSLv2 protocol and supports one or more ciphers.	
Impact An attacker might be able to use the known cryptographic flaws to eavesdrop the connection between clients and the service to get access to sensitive data transfered within the secured connection.	
Solution It is recommended to disable the deprecated SSLv2 and/or SSLv3 protocols in favor of the TLSv1+ protocols. Please see the references for more information.	
Vulnerability Insight The SSLv2 and SSLv3 protocols containing known cryptographic flaws.	
Vulnerability Detection Method	

Check the used protocols of the services provided by this system. Details: Deprecated SSLv2 and SSLv3 Protocol Detection (OID: 1.3.6.1.4.1.25623.1.0.111012) Version used: $Revision: 1183 $

References

https://www.enisa.europa.eu/activities/identity-and-trust/library/deliverables/algorithms-key-sizes-and-parameters-report, https://bettercrypto.org/

2.2 - TCP timestamps

Low (CVSS: 2.6)
OID: 1.3.6.1.4.1.25623.1.0.80091

Summary

The remote host implements TCP timestamps and therefore allows to compute the uptime.

Affected Nodes

199.38.223.84

Vulnerability Detection Result

It was detected that the host implements RFC1323. The following timestamps were retrieved with a delay of 1 seconds in-between: Paket 1: 119783127 Paket 2: 119783238

Impact

A side effect of this feature is that the uptime of the remote host can sometimes be computed.

Solution

To disable TCP timestamps on linux add the line 'net.ipv4.tcp_timestamps = 0' to /etc/sysctl.conf. Execute 'sysctl -p' to apply the settings at runtime. To disable TCP timestamps on Windows execute 'netsh int tcp set global timestamps=disabled' Starting with Windows Server 2008 and Vista, the timestamp can not be completely disabled. The default behavior of the TCP/IP stack on this Systems is, to not use the Timestamp options when initiating TCP connections, but use them if the TCP peer that is initiating communication includes them in their synchronize (SYN) segment. See also: http://www.microsoft.com/en-us/download/details.aspx?id=9152

Vulnerability Insight

The remote host implements TCP timestamps, as defined by RFC1323.

Vulnerability Detection Method

Special IP packets are forged and sent with a little delay in between to the target IP. The responses are searched for a timestamps. If found, the timestamps are reported. Details: TCP timestamps (OID: 1.3.6.1.4.1.25623.1.0.80091) Version used: $Revision: 787 $

References

http://www.ietf.org/rfc/rfc1323.txt