











Report Summary	
User Name:	Chris Clausen
Login Name:	nlsa_cc
Company:	NCSA
User Role:	Unit Manager
Address:	1205 W. Clark St
City:	Urbana
State:	Illinois
Zip:	61801
Country:	United States of America
Created:	10/11/2016 at 13:16:39 (GMT)
Template Title:	Level 543 confirmed - exclude non-running kernels
Asset Groups:	NCSA - NDS Labs
IPs:	-
Sort by:	Host
Trend Analysis:	Last 1 week
Date Range:	October 04, 2016 - October 11, 2016
Active Hosts:	3
Hosts Matching Filters:	2

Summary of Vulnerabilities

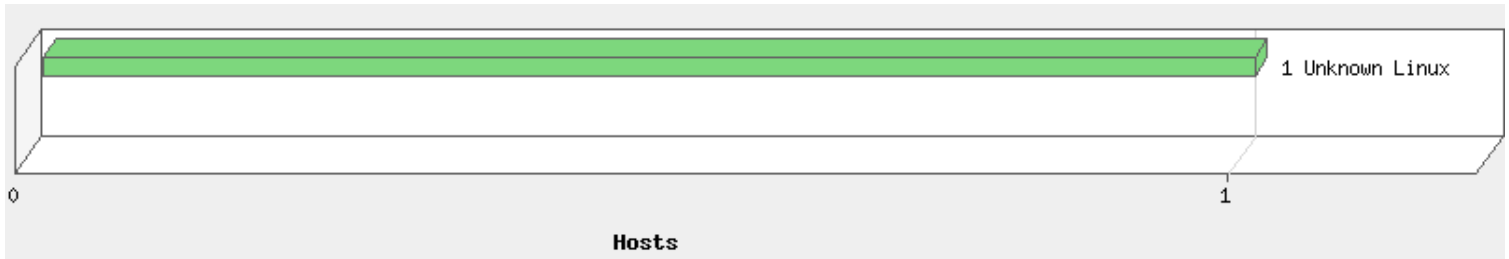
Vulnerabilities Total	6 (+6) 	Security Risk (Avg)	 3.0	Business Risk	 9/100
-----------------------	--	---------------------	---	---------------	---

by Status			
Status	Confirmed	Potential	Total
New	0	0	0
Active	6	0	6
Re-Opened	0	0	0
Total	6	0	6
Fixed	0	0	0
Changed	0	0	0

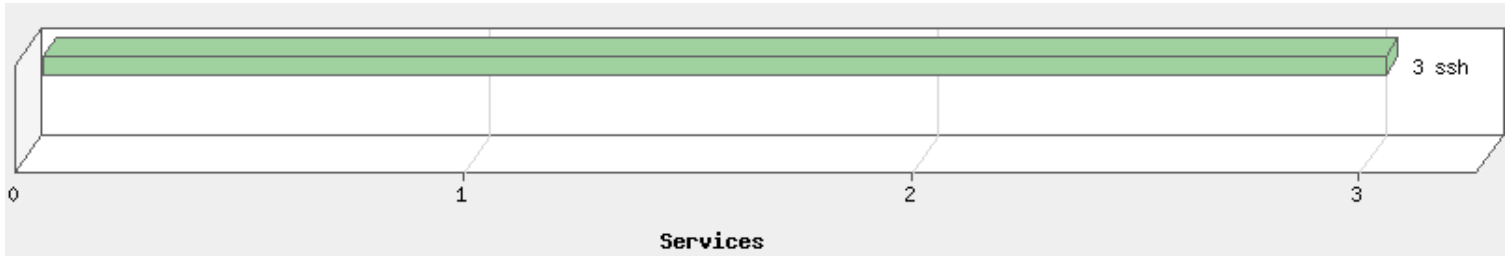
by Severity							
Severity	Confirmed	(Trend)	Potential	(Trend)	Information Gathered	Total	(Trend)
5	0	(0) -	0	(0) -	-	0	(0) -
4	0	(0) -	0	(0) -	-	0	(0) -
3	6	(+6) 	0	(0) -	-	6	(+6) 
2	0	(0) -	0	(0) -	-	0	(0) -
1	0	(0) -	0	(0) -	-	0	(0) -
Total	6	(+6) 	0	(0) -	-	6	(+6) 

5 Biggest Categories							
Category	Confirmed	(Trend)	Potential	(Trend)	Information Gathered	Total	(Trend)
General remote services	5	(+5) 	0	(0) -	-	5	(+5) 
Security Policy	1	(+1) 	0	(0) -	-	1	(+1) 
Total	6	(+6) 	0	(0) -	-	6	(+6) 

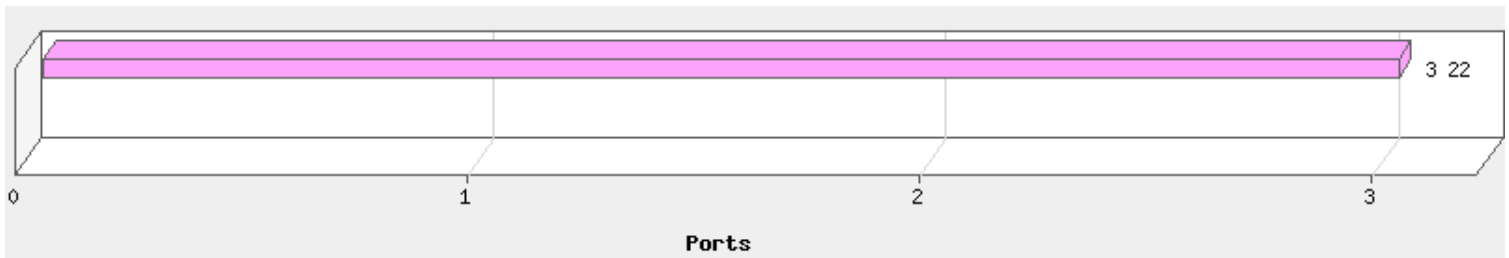
Operating Systems Detected



Services Detected



Ports Detected



Detailed Results

141.142.210.100 (*.workbench.nationaldataservice.org, -)

Unknown Linux

Vulnerabilities (2)

3 File Permissions (passwd, shadow and group) Are Not Properly Set

Active

QID: 105144
Category: Security Policy
CVE ID: -
Vendor Reference: -
Bugtraq ID: -
Service Modified: 05/21/2009
User Modified: -
Edited: No
PCI Vuln: Yes
Ticket State:

First Detected: 10/10/2016 at 20:24:20 (GMT)
Last Detected: 10/11/2016 at 12:06:08 (GMT)
Times Detected: 2
Last Fixed: N/A

THREAT:

File permissions for multiple files are not properly set. The "/etc/passwd" and "/etc/group" files should not have world or group writable permissions. The "/etc/shadow" file should not have world or group read/write permissions.

IMPACT:

As a result, malicious users may be able to modify the main system files and gain unauthorized access.

SOLUTION:

Properly set the file permissions for passwd, group and shadow.

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

/etc/shadow

-rw-r-----. 1 root root 161 Oct 10 09:48 /etc/shadow

 3 SSL/TLS Server supports TLSv1.0

port 443/tcp over SSL Active

QID:	38628
Category:	General remote services
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Service Modified:	07/14/2016
User Modified:	-
Edited:	No
PCI Vuln:	No
Ticket State:	

First Detected: 10/07/2016 at 15:08:07 (GMT)

Last Detected: 10/10/2016 at 19:38:08 (GMT)

Times Detected: 4

Last Fixed: N/A

THREAT:

TLS is capable of using a multitude of ciphers (algorithms) to create the public and private key pairs. For example if TLSv1.0 uses either the RC4 stream cipher, or a block cipher in CBC mode. RC4 is known to have biases and the block cipher in CBC mode is vulnerable to the POODLE attack. TLSv1.0, if configured to use the same cipher suites as SSLv3, includes a means by which a TLS implementation can downgrade the connection to SSL v3.0, thus weakening security. A POODLE-type (<https://blog.qualys.com/ssllabs/2014/12/08/poodle-bites-tls>) attack could also be launched directly at TLS without negotiating a downgrade.

This QID will be marked as a Fail for PCI as of November 1st, 2016 in accordance with the new standards. For existing implementations, Merchants will be able to submit a PCI False Positive / Exception Request and provide proof of their Risk Mitigation and Migration Plan, which will result in a pass for PCI up until June 30th, 2018.

Further details can be found at: NEW PCI DSS v3.2 and Migrating from SSL and Early TLS v1.1 (<https://community.qualys.com/message/34120>)

IMPACT:

An attacker can exploit cryptographic flaws to conduct man-in-the-middle type attacks or to decryption communications. For example: An attacker could force a downgrade from the TLS protocol to the older SSLv3.0 protocol and exploit the POODLE vulnerability, read secure communications or maliciously modify messages. A POODLE-type (<https://blog.qualys.com/ssllabs/2014/12/08/poodle-bites-tls>) attack could also be launched directly at TLS without negotiating a downgrade.

SOLUTION:

Disable the use of TLSv1.0 protocol in favor of a cryptographically stronger protocol such as TLSv1.2.

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

TLSv1.0 is supported

141.142.210.172 (*.test.nationaldataservice.org, -)

Vulnerabilities (4)



3 SSL/TLS Server supports TLSv1.0

port 443/tcp over SSL Active

QID: 38628
Category: General remote services
CVE ID: -
Vendor Reference: -
Bugtraq ID: -
Service Modified: 07/14/2016
User Modified: -
Edited: No
PCI Vuln: No
Ticket State:

First Detected: 10/04/2016 at 16:08:12 (GMT)
Last Detected: 10/10/2016 at 19:38:08 (GMT)
Times Detected: 8
Last Fixed: N/A

THREAT:

TLS is capable of using a multitude of ciphers (algorithms) to create the public and private key pairs. For example if TLSv1.0 uses either the RC4 stream cipher, or a block cipher in CBC mode. RC4 is known to have biases and the block cipher in CBC mode is vulnerable to the POODLE attack. TLSv1.0, if configured to use the same cipher suites as SSLv3, includes a means by which a TLS implementation can downgrade the connection to SSL v3.0, thus weakening security. A POODLE-type (<https://blog.qualys.com/ssllabs/2014/12/08/poodle-bites-tls>) attack could also be launched directly at TLS without negotiating a downgrade. This QID will be marked as a Fail for PCI as of November 1st, 2016 in accordance with the new standards. For existing implementations, Merchants will be able to submit a PCI False Positive / Exception Request and provide proof of their Risk Mitigation and Migration Plan, which will result in a pass for PCI up until June 30th, 2018. Further details can be found at: NEW PCI DSS v3.2 and Migrating from SSL and Early TLS v1.1 (<https://community.qualys.com/message/34120>)

IMPACT:

An attacker can exploit cryptographic flaws to conduct man-in-the-middle type attacks or to decryption communications. For example: An attacker could force a downgrade from the TLS protocol to the older SSLv3.0 protocol and exploit the POODLE vulnerability, read secure communications or maliciously modify messages. A POODLE-type (<https://blog.qualys.com/ssllabs/2014/12/08/poodle-bites-tls>) attack could also be launched directly at TLS without negotiating a downgrade.

SOLUTION:

Disable the use of TLSv1.0 protocol in favor of a cryptographically stronger protocol such as TLSv1.2.

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

TLSv1.0 is supported

 3 SSL/TLS Server supports TLSv1.0

port 10250/tcp over SSL **Active**

QID: 38628
Category: General remote services
CVE ID: -
Vendor Reference: -
Bugtraq ID: -
Service Modified: 07/14/2016
User Modified: -
Edited: No
PCI Vuln: No
Ticket State:

First Detected: 10/04/2016 at 16:08:12 (GMT)
Last Detected: 10/10/2016 at 19:38:08 (GMT)
Times Detected: 8
Last Fixed: N/A

THREAT:

TLS is capable of using a multitude of ciphers (algorithms) to create the public and private key pairs. For example if TLSv1.0 uses either the RC4 stream cipher, or a block cipher in CBC mode. RC4 is known to have biases and the block cipher in CBC mode is vulnerable to the POODLE attack. TLSv1.0, if configured to use the same cipher suites as SSLv3, includes a means by which a TLS implementation can downgrade the connection to SSL v3.0, thus weakening security. A POODLE-type (<https://blog.qualys.com/ssllabs/2014/12/08/poodle-bites-tls>) attack could also be launched directly at TLS without negotiating a downgrade. This QID will be marked as a Fail for PCI as of November 1st, 2016 in accordance with the new standards. For existing implementations, Merchants will be able to submit a PCI False Positive / Exception Request and provide proof of their Risk Mitigation and Migration Plan, which will result in a pass for PCI up until June 30th, 2018. Further details can be found at: [NEW PCI DSS v3.2 and Migrating from SSL and Early TLS v1.1 \(https://community.qualys.com/message/34120\)](https://community.qualys.com/message/34120)

IMPACT:

An attacker can exploit cryptographic flaws to conduct man-in-the-middle type attacks or to decryption communications. For example: An attacker could force a downgrade from the TLS protocol to the older SSLv3.0 protocol and exploit the POODLE vulnerability, read secure communications or maliciously modify messages. A POODLE-type (<https://blog.qualys.com/ssllabs/2014/12/08/poodle-bites-tls>) attack could also be launched directly at TLS without negotiating a downgrade.

SOLUTION:

Disable the use of TLSv1.0 protocol in favor of a cryptographically stronger protocol such as TLSv1.2.

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

TLSv1.0 is supported



3 SSL/TLS use of weak RC4 cipher

port 10250/tcp over SSL **Active**

QID: 38601
 Category: General remote services
 CVE ID: [CVE-2013-2566](#), [CVE-2015-2808](#)
 Vendor Reference: -
 Bugtraq ID: [91787](#)
 Service Modified: 01/29/2016
 User Modified: -
 Edited: No
 PCI Vuln: No
 Ticket State:

First Detected: 10/04/2016 at 16:08:12 (GMT)

Last Detected: 10/10/2016 at 19:38:08 (GMT)

Times Detected: 8

Last Fixed: N/A

THREAT:

Secure Sockets Layer (SSL v2/v3) and Transport Layer Security (TLS) protocols provide integrity, confidentiality and authenticity services to other protocols that lack these features.

SSL/TLS protocols use ciphers such as AES,DES, 3DES and RC4 to encrypt the content of the higher layer protocols and thus provide the confidentiality service. Normally the output of an encryption process is a sequence of random looking bytes. It was known that RC4 output has some bias in the output. Recently a group of researchers has discovered that there is a stronger bias in RC4, which make statistical analysis of ciphertext more practical.

The described attack is to inject a malicious javascript into the victim's browser that would ensure that there are multiple connections being established with a target website and the same HTTP cookie is sent multiple times to the website in encrypted form. This provides the attacker a large set of ciphertext samples, that can be used for statistical analysis.

NOTE: On 3/12/15 NVD changed the CVSS v2 access complicity from high to medium. As a result Qualys revised the CVSS score to 4.3 immediately. On 5/4/15 Qualys is also revising the severity to level 3.

IMPACT:

If this attack is carried out and an HTTP cookie is recovered, then the attacker can use the cookie to impersonate the user whose cookie was recovered.

This attack is not very practical as it requires the attacker to have access to millions of samples of ciphertext, but there are certain assumptions that an attacker can make to improve the chances of recovering the cleartext from ciphertext. For examples HTTP cookies are either base64 encoded or hex digits. This information can help the attacker in their efforts to recover the cookie.

SOLUTION:

RC4 should not be used where possible. One reason that RC4 was still being used was BEAST and Lucky13 attacks against CBC mode ciphers in SSL and TLS. However, TLSv 1.2 or later address these issues.

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

CIPHER	KEY-EXCHANGE	AUTHENTICATION	MAC	ENCRYPTION(KEY-STRENGTH)	GRADE
TLSv1 WITH RC4 CIPHERs IS SUPPORTED					
RC4-SHA	RSA	RSA		SHA1 RC4(128)	MEDIUM
TLSv1.1 WITH RC4 CIPHERs IS SUPPORTED					
RC4-SHA	RSA	RSA		SHA1 RC4(128)	MEDIUM
TLSv1.2 WITH RC4 CIPHERs IS SUPPORTED					



3 SSLv3.0/TLSv1.0 Protocol Weak CBC Mode Server Side Vulnerability (BEAST)

port 10250/tcp over SSL Active

QID: 42366
Category: General remote services
CVE ID: [CVE-2011-3389](#)
Vendor Reference: -
Bugtraq ID: [49388](#), [49778](#)
Service Modified: 07/22/2015
User Modified: -
Edited: No
PCI Vuln: No
Ticket State:

First Detected: 10/04/2016 at 16:08:12 (GMT)

Last Detected: 10/10/2016 at 19:38:08 (GMT)

Times Detected: 8

Last Fixed: N/A

THREAT:

SSLv 3.0 and TLS v1.0 protocols are used to provide integrity, authenticity and privacy to other protocols such as HTTP and LDAP. They provide these services by using encryption for privacy, x509 certificates for authenticity and one-way hash functions for integrity. To encrypt data SSL and TLS can use block ciphers, which are encryption algorithms that can encrypt only a fixed block of original data to an encrypted block of the same size. Note that these ciphers will always obtain the same resulting block for the same original block of data. To achieve difference in the output the output of encryption is XORed with yet another block of the same size referred to as initialization vectors (IV). A special mode of operation for block ciphers known as CBC (cipher block chaining) uses one IV for the initial block and the result of the previous block for each subsequent block to obtain difference in the output of block cipher encryption.

In SSLv3.0 and TLSv1.0 implementation the choice CBC mode usage was poor because the entire traffic shares one CBC session with single set of initial IVs. The rest of the IV are as mentioned above results of the encryption of the previous blocks. The subsequent IV are available to the eavesdroppers. This allows an attacker with the capability to inject arbitrary traffic into the plain-text stream (to be encrypted by the client) to verify their guess of the plain-text preceding the injected block. If the attackers guess is correct then the output of the encryption will be the same for two blocks.

For low entropy data it is possible to guess the plain-text block with relatively few number of attempts. For example for data that has 1000 possibilities the number of attempts can be 500.

For more information please see a paper by Gregory V. Bard. (<http://eprint.iacr.org/2006/136.pdf>)

NOTE:

The CVSS access complexity assigned by NIST to CVE-2011-3389 is 'Medium' which makes the base score 4.3. But Qualys has assigned access complexity to 'High' for server side, because Javascript injection and MiTM capabilities and a vulnerable client are required to exploit this vulnerability. Therefore the Qualys CVSS score is 2.6.

IMPACT:

Recently attacks against the web authentication cookies have been described which used this vulnerability. If the authentication cookie is guessed by the attacker then the attacker can impersonate the legitimate user on the Web site which accepts the authentication cookie.

SOLUTION:

This attack was identified in 2004 and later revisions of TLS protocol which contain a fix for this. If possible, upgrade to TLSv1.1 or TLSv1.2. If upgrading to TLSv1.1 or TLSv1.2 is not possible, then disabling CBC mode ciphers will remove the vulnerability.

Setting your SSL server to prioritize RC4 ciphers mitigates this vulnerability. Microsoft has posted information including workarounds for IIS at KB2588513 (<http://technet.microsoft.com/en-us/security/advisory/2588513>).

Using the following SSL configuration in Apache mitigates this vulnerability:

```
SSLHonorCipherOrder On
```

```
SSLCipherSuite RC4-SHA:HIGH:!ADH
```

Qualys SSL/TLS Deployment Best Practices can be found here (<https://www.ssllabs.com/projects/best-practices/>).

Note: RC4 recommendation is only in situations where upgrade to TLSv1.2 is not possible. RC4 in TLS v1.0 has output bias problem as described in QID 38601. Therefore it is recommended to upgrade to TLS v1.2 or later.

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

Available non CBC cipher	Server's choice	SSL version
RC4-SHA	ECDHE-RSA-DES-CBC3-SHA	TLSv1

CONFIDENTIAL AND PROPRIETARY INFORMATION.

Qualys provides the QualysGuard Service "As Is," without any warranty of any kind. Qualys makes no warranty that the information contained in this report is complete or error-free. Copyright 2016, Qualys, Inc.