FONDAZIONE
BRUNO KESSLER

CENTER FOR
CYBERSECURITY

Target: localhost:4444

Analysis performed on 2025-10-29 16:42

TLSAssistant

Version 3.1.0

Confidentiality Disclaimer

This report contains confidential information intended solely for the use of the individual or entity to whom it is addressed. If you are not the intended recipient, please be advised that any disclosure, copying, distribution, or use of the contents of this report is strictly prohibited. If you have received this report in error, please notify the sender immediately and delete the original message.

Security Tool Report Disclaimer

The information provided in this report is the result of security testing conducted by [Your Company/Organization] using TLSAssistant. The purpose of this tool is to assess the security of TLS configurations. The findings and recommendations presented in this report are based on the specific conditions and configurations tested at the time of the assessment. We respectfully recommend verifying the identified vulnerability thoroughly.

No Warranty or Guarantee

This report is provided "as is," without any warranty, express or implied, concerning the accuracy, completeness, legal value or reliability of the information contained herein. [Your Company/Organization] disclaims all warranties, including but not limited to, the implied warranties of merchantability and fitness for a particular purpose.

By reviewing this report, you acknowledge and agree to the terms and conditions outlined above.

Recap

Modules	**localhost:4444**
Bar Mitzvah	**Potentially Vulnerable**
RC4 NOMORE	**Potentially Vulnerable**

Detected vulnerabilities

localhost:4444

Bar Mitzvah

CVE:2015-2808 - CVSS2:4.3 (Medium)

By exploiting the invariance weakness of the RC4 stream cipher, an attacker is able to retrieve the session cookie by guessing the LSBs (least significant bits) of the keystream. After a phase in which the attacker sniffs the connection between two parties, it detects a weak key usage and tries to exploit the weakness.

Mitigation

Textual

Disable the RC4 stream cipher.

Apache

1. open your Apache configuration file (default:
/etc/apache2/sites-available/default-ssl.conf);
2. find the line starting with: SSLCipherSuite;
3. add the string :!RC4 at the end.

N.B. restart the server by typing: sudo service apache2 restart.

nginx

1. In a default situation, you can edit your website configuration
/etc/nginx/sites-enabled/default
(if you changed your site conf name
/etc/nginx/sites-enabled/YOURSITECONFIGURATION);
2. Inside server {...} brackets configuration, find ssl_ciphers;
3. Remove RC4 (if any) and add :!RC4 at the end.

N.B. restart the server by typing: sudo service nginx restart.

RC4 NOMORE

CVE:Not available - CVSS3:Not available

RC4 Numerous Occurrence MOnitoring & Recovery Exploit

Given the biases existing in the key generation algorithm, an attacker can use statistics to guess information. The capture of the session cookie is operated by surrounding the token itself with known plaintext and repeatedly connecting to the server. After *collecting a fair amount of packets, the attacker can exploit the biases to calculate the cookie.*

Mitigation

Textual

Disable the RC4 stream cipher.

Apache

1. open your Apache configuration file (default: *`/etc/apache2/sites-available/default-ssl.conf`*);
2. find the line starting with: SSLCipherSuite;
3. add the string `:!RC4` at the end.

N.B. restart the server by typing: `sudo service apache2 restart`.

nginx

1. In a default situation, you can edit your website configuration *`/etc/nginx/sites-enabled/default`* (if you changed your site conf name *`/etc/nginx/sites-enabled/YOURSITECONFIGURATION`*);
2. Inside `server {...}` brackets configuration, find `ssl_ciphers`;
3. Remove `RC4` (if any) and add `:!RC4` at the end.

N.B. restart the server by typing: `sudo service nginx restart`.