FEBRUARY 2015

Citrix NetScaler Platinum Edition and Citrix Receiver

Product Description

The Citrix NetScaler Platinum Edition, henceforth known as the NetScaler, is a rack mounted network gateway hardware device. A typical deployment uses features such as Load Balancing, NetScaler Gateway, Web Application Firewall, Global Server Load Balancing and Authentication, Authorisation and Auditing for application traffic. This evaluation looked at the NetScaler's role in Transport Layer Security (TLS) connections.

Citrix Receiver is the client software used for accessing content served by Citrix XenApp, Citrix Desktop or Citrix Storefront. This evaluation looks at the Receiver's role in TLS connections. ASD has evaluated the following product versions:

- NetScaler 10.0 –all builds.
- NetScaler 10.1 up to and including build 123.11.e.nc
- NetScaler 10.5 (Excluding Elliptic Curve functionality[1])
- NetScaler MPX 5550, MPX 5650, MPX 5750, MPX 7500, MPX 8005, MPX 8015, MPX 8200, MPX 8400, MPX 8600, MPX 8800, MPX 10500, MPX 11500, MPX 11515, MPX 11520, MPX 11530, MPX 11540, MPX 11543, MPX 12500, MPX 13500, MPX 14500, MPX 16500, MPX 17550, MPX 18500, MPX 19500, MPX 19550, MPX 20500, MPX 20550, MPX 21500, MPX 21550, MPX 22040, MPX 22060, MPX 22080, MPX 22120
- Receiver versions 3.3, 3.4, 4.0 and 4.1 for Windows.

Evaluation Scope

The ACE focussed on the TLS VPN formed between the NetScaler and Receiver and does not include the NetScaler VPX platforms. The following functionality was investigated:

- Key generation on the NetScaler.
- Key generation on the Receiver.
- TLS endpoint configuration.
- Data transit between the Receiver and NetScaler.
- Authentication methods.

[1] ASD has not evaluated any Elliptic Curve functionality in this product.

Common Criteria Certification - Summary

At the time of this Consumer Guide's publication:

- Citrix NetScaler Platinum Edition 10.0 has completed a Common Criteria (CC) evaluation at the EAL 2+ level.
- Citrix NetScaler Platinum Edition 10.1 did not undergo CC evaluation.
- Citrix NetScaler Platinum Edition 10.5 is at the time of publication currently undergoing CC evaluation in the United Kingdom.

ASD has waived the requirement for a CC evaluation for the NetScaler version 10.1 and 10.5.

The VPN formed by the Receiver and NetScaler may still be used in accordance with this consumer guide.

ASD Findings and Recommendations

1. The TLS VPN formed between the Citrix NetScaler Platinum Edition and Citrix Receiver when appropriately configured was found to be suitable for enabling the secure transfer of PROTECTED information across an UNCLASSIFIED network in accordance with the Cryptography section of the Information Security Manual (ISM).

2. The configuration advice given below applies to the virtual server on the NetScaler specifically being used to handle connections with the Receiver.

3. To conform to the Cryptography section of the ISM, the NetScaler must be configured such that the only CipherSuites it will accept are:

    a. TLS-AES-128-CBC-SHA
    b. TLS-AES-256-CBC-SHA
    c. TLS-DHE-RSA-AES-128-CBC-SHA
    d. TLS-DHE-RSA-AES-256-CBC-SHA

4. RSA key generation and certificate generation can be performed on the NetScaler. RSA keys for certificates should be generated either on the NetScaler, or externally by a source approved for PROTECTED.

5. It should be noted that the NetScaler cannot perform DSA operations, and therefore DSA server certificates cannot be used.

6. The Receiver must be run in its stand-alone form, and must not be launched or accessed from a web browser.

7. Agencies must use two-factor authentication for remote user authentication.

8. Agencies must disable all forms of TLS renegotiation on the NetScaler.

9. The client device with the Receiver must be considered a PROTECTED device upon its first contact with a PROTECTED remote desktop. This does not necessarily preclude BYOD solutions. See "Using Remote Desktop Clients" (December 2011) for advice on how to reduce the risk of uncontrolled devices leaking PROTECTED data.

10. Note that while the NetScaler supports up to TLS 1.2, the Receiver only supports up to TLS 1.0. Therefore the VPN that forms between any of the approved NetScalers and Receivers will use TLS 1.0.

11. Note that the use of client certificates requires an RSA card reader for the stand alone Receiver client.

12. Contact ASD for advice on any potential use of NetScaler MPX devices not listed here.

Contact Details

Australian government customers with questions regarding this advice should contact ASD Advice and Assistance at asd.assist@defence.gov.au or by calling 1300 CYBER1 (1300 292 371).

ISM

The advice given in this document is in accordance with the Information Security Manual 2014. Australian Government agencies are reminded to periodically check the latest release date of the ISM at http://www.asd.gov.au/infosec/ism/index.htm

Consumer Guide

This Consumer Guide was updated on 10th February 2015.