NSE

Circular

National Stock Exchange Of India Limited

Department : MEMBER SERVICE DEPARTMENT	
Download Ref No: NSE/MSD/42115	Date : September 12, 2019
Circular Ref. No: 46/2019	

All Members

Decommissioning of support for TLS 1.0 & TLS 1.1 for web-based applications

To enhance the security of data and communications to and from NSE web-based systems, we intend to decommission the support for TLS 1.0 and TLS 1.1 protocols for following web based applications:

1. NSE E-IPO (www.nseindiaipo.com)
2. EBP - Electronic Bidding Platform (www.nse-ebp.com)
3. CBRICS – Corporate Bond Reporting Platform (www.bricsonline.net)
4. EBID – Electronic bidding (www.nse-ebid.com)

TLS (Transport Layer Security) is the protocol which secures HTTPS. TLS provides secure communication between web browsers and servers. TLS 1.2 was published ten years ago to address weaknesses in TLS 1.0 and 1.1 and has enjoyed wide adoption since then.

Accordingly, the leading browsers have decided to drop the support for the earlier versions of the protocol i.e. TLS 1.0 and TLS 1.1.

1. Microsoft will disable Transport Layer Security (TLS) 1.0 and 1.1 by default in supported versions of Microsoft Edge and Internet Explorer 11 in the first half of 2020.
2. Firefox will disable support for TLS 1.0 and TLS 1.1 in March 2020
3. Google Chrome will disable support for TLS 1.0 and TLS 1.1 in Chrome 72. TLS 1.0 and 1.1 will be disabled altogether in Chrome 81. This will affect users on early release channels starting January 2020.

With this background, and considering the implications, all members are requested to implement **one** of the following:

1. Upgrade the browsers to the latest versions.
   a. Google's Chrome - https://www.google.com/chrome/
   b. Mozilla's Firefox - https://www.mozilla.org/en-US/firefox/new/
   c. Microsoft's Internet Explorer http://windows.microsoft.com/enus/internetexplorer/download-ie
   d. Microsoft's Edge – https://www.microsoft.com/enus/download/details.aspx?id=48126
2. Update the settings as per the steps outlined in Annexure - 1.
3. For members connecting to the application using any other variant of clients (like for making API call), members are requested to check and make necessary changes at their end so that client supports connections over TLS 1.2.

This circular shall be applicable w.e.f October 1, 2019, for web facing applications/websites and only accept connections over TLS 1.2 version.

Reference Links:

1. https://blogs.windows.com/msedgedev/2018/10/15/modernizing-tls-edgeie11/#Qt07jVdqb5lj99jy.97
2. https://security.googleblog.com/2018/10/modernizing-transport-security.html
3. https://www.ssl.com/article/tls-1-3-is-here-to-stay/
4. https://blog.mozilla.org/security/2018/10/15/removing-old-versions-of-tls/
5. https://kinsta.com/blog/tls-1-3/

Disclaimer:

1. The information contained in this notice has been extracted from the reference links as above
2. Members shall act upon this notice at their own discretion after conducting appropriate impact/risk analysis to their specific environment. Please test all the settings in a test environment before being deployed on production.

For and on behalf of
National Stock Exchange of India Limited

Abhijeet Sontakke
Chief Manager

Toll Free No	Fax No	Email id
1800-266-0053	+91-22-26598449	msm@nse.co.in