I/563030/2022

Government of India
Ministry of Finance, Department of Revenue
Central Board of Indirect Taxes & Customs
Directorate General of Human Resource Development, HRM-I
Bhai Vir Singh Sahitya Sadan, 2nd & 3rd Floor, Bhai Vir Singh Marg
Gole Market, New Delhi-110 001
Telephone No. 011-23340315

Dated the 12th April, 2022

To,

The Pr. Chief Commissioner / Chief Commissioner of Customs and GST (All),
The Pr. Director General / Director General (All),
The Pr. Commissioner / Commissioner I/C of Directorates (All),
The Pr. Commissioner / Commissioner, Settlement Commission (All),
The Pr. Commissioner / Commissioner, CESTAT (All),

Subject: Advisory for Cyber Attacks on Railtel Network –reg.

Sir/ Madam,

We have received a high alert advisory from Cert-In and Railtel regarding possible credential leak of a CBIC VPN user (edgevpn.rcil.gov.in.).

In this regard, it is informed that the CBIC VPN Module is a critical entity and may also be on the target list of cyber attackers. Any such leakage may jeopardize the data integrity and may lead to unauthorized access to internal information.

In the view of advisory from Cert-in, it is requested to advise your field formations to be vigilant & proactive and to report us and Cert-in in case of any security incident.

Further, the recommendations to be adhered to strictly (in addition to any other security measures being already taken by your organization) are as under:

1. Passwords must be changed and should be strong for all the machines managed by Officers. Password should at least adhere to the basic security hygiene by using a combination of letters, numbers, and characters. It shouldn't be shared with any other account.
2. Default User name password provided by OEM must be changed in all the

systems used by Officers.

3. Admin access must be restricted and should be with only limited technical officers.

4. Machines that are being used to access the VMs must be secured with updated antivirus.

5. VPN must be used to access the e-office and while working from home. The VPN password must be strong and must not be shared with others.

6. Public Websites must be audited(including Source Code review) by Cert-in and must be kept behind WAF (web access firewall). You may contact the SPARROW-CBIC team for any support on WAF part at email Id- help.sparrow.cbic@gov.in.

Yours Faithfully,

(Santosh Kumar Mishra)
Additional Director
HRM-I, DGHRD