O/o The Principal General Manager
(Broadband Networks , Bangalore)

भारत संचार निगम लिमिटेड
(भारत सरकार का उपक्रम)
BHARAT SANCHAR NIGAM LIMITED
(A Govt. of India Enterprise)
Broadband Network Circle

No: PGM/BBNW/FTTH/2019-20/55 Dated 20.02.2020

CRITICAL

To
All SSA Heads, BSNL

Sub: Action to be taken by SSAs to attend the Security risk caused by improperly configured Third Party ONTs

Ref: 1. DO No:CMD/BSNL/Broadband/2017-18 Dated 25-10-2017
2. PGM/BBNW/MULTIPLAY/2017-18 DATED 26.07.2017
3. PGM/BBNW/MULTIPLAY/2017-18 DATED 05.08.2017
4. BSNL/BBNW/BG/P3/BOTNET/2017/05 DATED 01.08.2017
5. PGM/BBNW/TECH/2017-18 DATED 07.08.2017
6. PGM/BBNW/FTTH/2017-18 DATED 05.09.2017
7. PGM/BBNW/ISC/2017-18/ dated 31.10.2017
8. 2-1/2013/UDS dtd 07-05-2015 from DoT

Security measures to be adopted in FTTH ONTs/ ONTs to safeguard against misuse have been communicated to all the stake holders - Circle coordinators, Node in charges, Field units, Broadband customers and NOC units from this office vide letters at ref 2 to 7 above from time to time. These guidelines are also informed during the integration of Third Party OLTs in BSNL Network. It is observed that the security measures provided are not being followed by the Third party service provider in their ONTs and ~~are~~ these ONTs are becoming a potential threat to network breach.

It is requested to follow the security guidelines given in Annexure-1 for the end user internet connected ONTs, especially Third party ONTs.

In this context to avoid possible Security risk caused by improperly configured end user internet connected devices CPEs,(FFTH ONTs and TIP ONTs) BBNW NOC, on a proactive basis is publishing the list of user who are having default passwords and WAN side vulnerable ports open on the intranet regularly. SSAs are requested to take the above mentioned necessary steps and help in proper configuration of end devices by assisting the identified users.

All the SSA heads/Circle coordinators are hereby requested to depute the staff/officers/TIP operators to the customer premises and to guide the customers to attend to these vulnerable devices immediately as per the procedure which will ensure the safety & security of the customer devices.

A report on cleared cases shall be sent to this office by FAX/mail. The status of the cases after taking necessary action along with resolved/pending shall be communicated/updated in the NOC records/systems.

Thankyou very much for your support & co-operation.

(D.M.EZHIL BUDDHAN)
Principal General Manager
Broadband Networks
Bangalore – 560 005

प्रधान महाप्रबंधक
PRINCIPAL GENERAL MANAGER
ब्रॉडबैंड नेटवर्क, बीएसएनएल
Broadband Networks, BSNL
पाँचवी मंजिल, दीपी पूर्व टेलीफोन एक्सचेंज भवन
5th Floor, DPE East Telephone Exchange Bldg.
लेजर रोड, बेंगलूर-५६० ००५
Lazer Road, Bangalore-560 005

Copy to: 1. All CGMs of Telecom circles/Telecom Districts for kind information pl.
2. CGM, BBNW, New Delhi for kind information pl.
3. PGM(NWO-BB/IN) BSNL CO for kind information pl.
4. GM (NWP-BB), BSNLCO, New Delhi for kind information pl.
5. GM (CIT)/CISO,BSNL for kind information pl.

5th Floor, Bangalore East Telephone Exchange, Lazar Road, Bangalore East, Bangalore 560005.
Tel. No: 080- 2580 8890, Fax: 080 – 2580 8880, Mob: + 91 94480 10361. Email: buddhan@bsnl.co.in

O/o The Principal General Manager
(Broadband Networks , Bangalore)

भारत सचार निगम लिमिटेड
(भारत सरकार का उपक्रम)
BHARAT SANCHAR NIGAM LIMITED
(A Govt. of India Enterprise)
Broadband Network Circle

ANNEXURE-1

1. Node in charges/Field units should ensure change of the default username/password to a strong password at the time of installation/ while attending ONT faults at customer site to avoid unauthorized access to ONT. Customers have been given instructions to change the password as well.
2. Node in charges/Field units should disable all vulnerable protocol ports on WAN side in TR-69 non-compliant ONTs.
3. Node incharges/Field units should to block all vulnerable ports which are open in FTTH ONTs/ TIP ONTs at customer end.
4. While activating TIP / FTTH connections, Filed units should ensure to disable CWMP port, FTP, TELNET, SSH, HTTP, SNMP, UPnP till ACS is made available. Upgrade all FTTH ONT/ TIP ONTs firmware with the latest one.
5. Circle heads to ensure that BSNL/TIP supplied ONTs are ITU-T, G.9980 standard complaint.
6. For the customer owned ONTs, Node incharges/Field units to ensure that those CPEs are ITU-T, G.9980 standard complaint. Also the same should be specified in Terms and conditions of Customer Application /Acquisition Form (CAF).
7. Field units should ensure that all vulnerable ports which are open in FTTH ONTs/ TIP ONTs are blocked during activation of connections, in case the CPEs are purchased by customers.
8. Node incharges/Field units should activate the FTTH connections only after vulnerable ports are blocked.
9. Field units should advice the customers at the time of installation/ while attending ONT faults to block the ports in the ONT on LAN side except HTTP (80) /HTTPS (443) for safety purpose. Since ONT administration login/password is with customer, they can modify/open any port on LAN side of ONT as per their need. Field units have been requested to intimate the customers to disable all WAN side access and enable ACL/ Firewall on all FTTH ONT/ TIP ONTs.
10. Field units should intimate the customers to change the default password again to the earlier password or any other new password whenever the reset button in the CPEs is operated.
11. Field units should advice the customers to switch off the ONT, when not in use.

5th Floor, Bangalore East Telephone Exchange, Lazar Road, Bangalore East, Bangalore 560005.
Tel. No: 080- 2580 8890, Fax: 080 - 2580 8880, Mob: + 91 94480 10361. Email: buddhan@bsnl.co.in