BLUE|LINE PASSWORD HACK FIX
SOLUTION FOR PASSWORD BACKDOOR

FOR IMMIDEATE RELEASE

PROBLEM

Recently, some end users informed us that their BLUE|LINE RECORDERS were hacked and could not function properly. We are responding instantly to provide solution to help our partners and end users to restore the affected products to normal use, while its protection level has also been improved.

Hackers made use of publicly known default value to remotely connect into storage devices which was still using default username/password, and changed channel name, image parameters to black out the device. To thwart future attacks, we are providing a solution to thoroughly address this problem:

SOLUTION

1. To restore a hacked recorder the user shall upgrade the device firmware to the latest version

2. Restore to factory default.

3. Change all password to more secure ones with digits, lower/upper case alphabets, symbols and no less than 8 length or follow the initialization procedure to change the default password. *(If you can't login or don't have new firmware, please contact your dedicated technical support contact for reset code or latest firmware.)*

4. Once defaulted for normal use, the customer shall change the default password, preferably a strong password to avoid being attacked. *(Do not forget to Write down the new ID and Password)*

5. To prevent your recorders in the best protected condition, we recommend upgrading to the latest firmware on a regular basis.

Call 631-396-0800   For Tech Support

WINIC