



Dear Valued Customer/Partner:

We were recently made aware of a cybersecurity vulnerability that affects a number of our recorders. It's important to note that, any hostile attack for this vulnerability will let NVR system die and cannot boot up if NVR connect to network

Our team of engineering and security specialists have been conducting exhaustive test and are developing a series of firmware patches to alleviate this issue along with the information you need to implement these proactive updates. Our technical team also will be available if you would like our assistance installing these firmware updated.

This update will for our NVR following models:

HiSilicon 3535 Series:

AE-N6001-36EH、 AE-N6001-25EH、 AE-N6000-16EFP、 AE-N6000-36EF、
AE-N6000-25EF、 AE-N6000-25EH、 AE-N6000-9EH、 AE-N6000-4EH、 AE-N6100-16EH、
AE-N6100-9EH、 AE-N6200-16EH、 AE-N6200-9EH、 AE-N6200-4EH、
AE-N6100-9EH-8P/48、 AE-N6100-4EHP/48

HiSilicon 3520D Series:

AE-N6200-8E、 AE-N6200-4E、 AE-N6100-4ET/15、 AE-N6100-4EP/48、
AE-N6100-8EP/48、 AE-N6200-4EL、 AE-N6200-8EL

We strongly suggest you do update firstly before using. Please rest assured that AEVISION has taken immediate action to address this situation and will continue to work towards implementing surveillance solutions that provide the highest levels of security and integrity.

AEVISION greatly appreciates your support and trust, and welcomes any feedback or questions you may have for our products

Thanks for your attention.

Guangzhou Aevison Electronics Technology Co., Ltd

29th, March, 2017