Privilege-Escalating Vulnerability Notice

March 20th, 2017

To our Valued Customers and Partners:

Northern recently became aware of a security vulnerability concerning Northern-Branded IP cameras which could potentially present a cybersecurity concern under certain circumstances. Northern is notifying you with this announcement that a firmware update will be required to remedy this potential issue. Upgrading to the latest firmware will resolve this issue.

Please note: The majority of Northern cameras mentioned above are accessed through a NVR, Northern iVMS software or other 3rd party VMS software. When connected in these manners, only a limited possibility exists for a camera to be open to direct public access, reducing the risk of cybersecurity exposure.

What is the privilege-escalating vulnerability?

When a specific request code is used to access the IP cameras with particular firmware versions directly, it may allow attackers to obtain an unauthorized escalated additional user privilege to acquire or tamper with the device information.

Which Northern products could be affected and how are those cameras accessed?

The Northern products which could be affected are as follows:

Product Series	Product Number	New Firmware
2 Megapixel Products	IPPTZ30XIR	v5.3.9 Build 170123
3 Megapixel Products	IP3B, IP3D, IP3T, IP3W, IP3VFD, IP3VFB	v5.3.0 Build 170316
4 Megapixel Products	IP4B, IP4D, IP4D4MM, IP4T, IP4W, IP4MVFD, IP4MVFB	v5.4.1 Build 170316

How is Northern resolving this issue?

In order to protect our valued customers from any threats, Northern is informing partners about the issue and making immediately available for download a firmware upgrade that resolves the issue on the affected cameras.

What should users of these cameras do?

Northern is advising and recommending all uses of these cameras to upgrade to the latest firmware which will fix this issue. The latest firmware is available for download on Northern's website homepage: www.northernvideo.com or by clicking on the New Firmware link in the table above for the appropriate product.

Northern believes it is our responsibility to keep all partners informed about any security threats that could affect our products and to also provide resolutions to address and fix any such issues as quickly as possible.

We thank you for your understanding and support in this matter.