VIVOTEK Product Security Advisory

Advisory ID: VVTK-SA-2018-004
CVE ID: CVE-2018-14769
First Published: August 24, 2018
Last Update: August 24, 2018
Status: Fixed
Revision: 1

Overview:

Security researcher Ayushman Dutta discovered that VIVOTEK Network Camera have Cross-Site Request Forgery (CSRF) vulnerability. It allows remote attackers to hijack the cgi command. For more CSRF information please check following URL: https://en.wikipedia.org/wiki/Cross-site_request_forgery.

Affect Products:

All Network Camera Series using firmware prior to XXXXXX-VVTK-0X06a.

Workarounds:

1. Using VMS (video management system) to manage your IP Camera device, as VMS is NOT affected or attacked by CSRF.
2. Avoid using operation system's default browser to manage your IP Camera. Since CSRF can only attack browsers that you have logged into for IP Cameras and trigger attacks by precision prepared malicious webpage, using a non-default browser can effectively reduce the risk of being attacked.

Solution:

Please upgrade firmware to XXXXXX-VVTK-0X06a or above.

Alert:

Due to CSRF protection solution, after upgraded you camera firmware, please also upgrade your Shepherd to version 3.0 or above to make all operations function normally.

Revision History:

Revision 1 / August 24, 2018 / Initial release