Cyber Security Advisory

Advisory ID: vvtk-sa-20170623-02
CVE ID: CVE-2017-9829
First Published: August 02, 2017
Last Update: November 10, 2017
Status: Fixed

Overview:

'/cgi-bin/admin/downloadMedias.cgi' of the web service in most of the VIVOTEK network cameras is vulnerable, which allows remote attackers to read any file on the Linux file system of the camera via a crafted HTTP request containing ".." sequences.

The vulnerability exists because the affected CGI does not sufficiently validate the file path.

The risk is low when the password is difficult to crack. It is highly recommended to configure a strong password for root and all administrator accounts.

Affected Products:

All VIVOTEK cameras.

Mitigation:

Make sure you have strong passwords for root and all administrator accounts.

Solution:

VIVOTEK has rolled out camera firmware* in July 2017 with downloadMedias.cgi that allows only the specific file path.

* Please refer to the model list below for firmware update.

Camera Models for Firmware Update:

CC8370-HV
CC8371-HV
CD8371-HNTV
CD8371-HNVF2
FD8166A
FD8166A-N
FD8167A
FD8167A-S
FD8169A
FD8169A-S
FD816BA-HF2
FD816BA-HT
FD816CA-HF2
FD8177-H
FD8179-H
FD8182-F2
FD8182-T
FD8366-V
FD8367A-V
FD8369A-V
FD836BA-EHTV
FD836BA-EHVF2
FD836BA-HTV
FD836BA-HVF2
FD8377-HV
FD8379-HV
FD8382-ETV
FD8382-EVF2
FD8382-TV
FD8382-VF2
FD9171-HT
FD9181-HT
FD9371-EHTV
FD9371-HTV
FD9381-EHTV

FD9381-HTV

FE8182

FE9181-H

FE9182-H

FE9191

FE9381-EHV

FE9382-EHV

FE9391-EV

IB8360-W

IB8367A

IB8369A

IB836BA-EHF3

IB836BA-EHT

IB836BA-HF3

IB836BA-HT

IB8377-H

IB8379-H

IB8382-EF3

IB8382-ET

IB8382-F3

IB8382-T

IB9371-EHT

IB9371-HT

IB9381-EHT

IB9381-HT

IP8166

IP9171-HP

IP9181-H

IZ9361-EH

MD8563-EHF2

MD8563-EHF4

MD8563-HF2

MD8563-HF4

MD8564-EH

MD8565-N

SD9161-H

SD9361-EHL

SD9362-EH

SD9362-EHL

SD9363-EHL

SD9364-EH

SD9364-EHL

SD9365-EHL

SD9366-EH

SD9366-EHL

VC8101

VS8100-v2