neolead / **CVE-2018-10988.txt**

Created a month ago

CVE-2018-10988

CVE-2018-10988.txt

```
CVE-2018-10988

[Suggested description]
An issue was discovered on Diqee360 devices (http://diqee.com).
A firmware update process, integrated into the firmware, starts at boot and tries to find the update folder on the microSD ca
It executes code, without a digital signature, as root from the
/mnt/sdcard/$PRO_NAME/upgrade.sh or /sdcard/upgrage_360/upgrade.sh pathname.
----------------------------------------

[Additional Information]
if [ -d "/mnt/sdcard/$PRO_NAME" ]; then  echo "/mnt/sdcard/$PRO_NAME
is exist..."
 cd /mnt/sdcard
 chmod 777 /mnt/nand1-2/$PRO_NAME/ -R
/mnt/sdcard/$PRO_NAME/upgrade.sh fi
----------------------------------------

[VulnerabilityType Other]
Insecure update process
----------------------------------------

[Vendor of Product]
Dongguan Diqee intelligent Co., Ltd.
----------------------------------------

[Affected Product Code Base]
Diqee360 - any
----------------------------------------

[Affected Component]
Update firmware without signification cause root access.
----------------------------------------

[Attack Type]
Local
----------------------------------------

[CVE Impact Other]
Insecure unsigned firmware update
----------------------------------------

[Attack Vectors]
Update process starts at boot and try to find update folder at
micro-sd card.So when boot up , diqee run as root user
/sdcard/upgrage_360/upgrade.sh without any sign code check.
Researchers put script to sd card into folder upgrage_360, insert sd
card to vacuum and restart it.
----------------------------------------

[Reference]
https://facebook.com/neolead
http://ptsecurity.com/
----------------------------------------

[Discoverer]
Leonid Krolle(Positive Technologies), George Zaytsev(Positive Technologies)
```