neolead / **CVE-2018-10987.txt**

Created a month ago

CVE-2018-10987

**CVE-2018-10987.txt**

```
CVE-2018-10987

[Suggested description]
An issue was discovered on Dongguan Diqee Diqee360 vacuum cleaner devices.
The affected vacuum cleaners suffers from an authenticated remote code
execution vulnerability. An authenticated attacker can send a
specially crafted UDP packet, and execute commands on the vacuum
cleaner as root. The bug is in the function REQUEST_SET_WIFIPASSWD (UDP command 153).
A crafted UDP packet runs "/mnt/skyeye/mode_switch.sh %s" with an
attacker controlling the %s variable. In some cases, authentication
can be achieved with the default password of 888888 for the admin account.
----------------------------------------

[Additional Information]
Requirements:
Must know the UID, must know login-password. Standard combination of
easy credentials: admin:888888 - A remote attacker can exploit this
issue and execute arbitrary system commands granting system access
with root privileges to get system shell.
----------------------------------------

[VulnerabilityType Other]
Remote code execution
----------------------------------------

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

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

[Affected Component]
Update wifi AP command
----------------------------------------

[Attack Type]
Remote
----------------------------------------

[Impact Code execution]
true
----------------------------------------

[Attack Vectors]
Authenticated attacker can send a specially crafted udp packet, and execute command on vacuum cleaner diqee 360 as root.
The bug are hide in function REQUEST_SET_WIFIPASSWD - udp command 153"
Special crafted udp packet runs /mnt/skyeye/mode_switch.sh %s, because attacker control %s variable.
----------------------------------------

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

[Has vendor confirmed or acknowledged the vulnerability?]
true
----------------------------------------

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

```