

# devolo dLAN Cockpit 4.3.1 Unquoted Service Path Privilege Escalation

2019-02-05 / 2019-02-04

Credit: [Stefan Petrushevski \(https://cxsecurity.com/author/Stefan+Petrushevski/1/\)](https://cxsecurity.com/author/Stefan+Petrushevski/1/)

Risk: Medium

Local: No

Remote: Yes

CVE: N/A

CWE: CWE-264  
(<https://cxsecurity.com/cwe/CWE-264>)

**devolo dLAN Cockpit 4.3.1 Unquoted Service Path Privilege Escalation**

**Vendor:** devolo AG  
**Product web page:** <https://www.devolo.com>  
**Affected version:** 4.3.1

**Summary:** devolo dLANA(r) Cockpit is a software tool that allows devolo customers to monitor and optimise their dLANA(r) network using a software tool.

**Desc:** The application suffers from an unquoted search path issue impacting the service 'DevoloNetworkService' for Windows deployed as part of Devolo dLANA(r) Cockpit software application. This could potentially allow an authorized but non-privileged local user to execute arbitrary code with elevated privileges on the system. A successful attempt would require the local user to be able to insert their code in the system root path undetected by the OS or other

security applications where it could potentially be executed during application startup or reboot. If successful, the local user's code would execute with the elevated privileges of the application.

Tested on: Microsoft Windows 7 Ultimate SP1 (EN)

Vulnerability discovered by Stefan Petrushevski aka sm  
@zeroscience

Advisory ID: ZSL-2019-5506

Advisory URL: <https://www.zeroscience.mk/en/vulnerabilities/ZSL-2019-5506.php>

04.10.2017

--

| ServiceName          | Path                          | StartName   |
|----------------------|-------------------------------|-------------|
| ame                  | AbuseFunction                 |             |
| -----                | ----                          | -----       |
| ---                  | -----                         |             |
| DevoloNetworkService | C:\Program Files\devolo\dl... | LocalSystem |
| system               | Write-ServiceBinary -Servi... |             |

C:\>sc qc DevoloNetworkService

[SC] QueryServiceConfig SUCCESS

SERVICE\_NAME: DevoloNetworkService

```

TYPE                : 110  WIN32_OWN_PROCESS (interactive)
START_TYPE          : 2    AUTO_START
ERROR_CONTROL       : 1    NORMAL
BINARY_PATH_NAME    : C:\Program Files (x86)\devolo\dlan\de

```

```
volonetsvc.exe
LOAD_ORDER_GROUP :
TAG : 0
DISPLAY_NAME : devolo Network Service
DEPENDENCIES :
SERVICE_START_NAME : LocalSystem
```

**See this note in RAW Version** (<https://cxsecurity.com/ascii/WLB-2019020037>).

Post



**Comment it here.**

---

**Nick (\*)**

**Email (\*)**

**Video**

**Text (\*)**

