liyansong2018 D-Link 2640 Disclosure of Sensitive Information ... on Jun 13, 2021 History

..

README.md last year

README.md

Plain Credentials in DIR-2640-US Router

Overview

- **CVE ID**: CVE-2021-34204
- **Type**: Insufficiently Protected Credentials - *(522)*
- **Vendor**: D-LINK (https://www.dlink.com/)
- **Products**: WiFi Router, such as DIR-2640-US.
- **Version**: Firmware (1.01B04)
- **Fix**: None

Severity

Medium 4.6 CVSS:3.1/AV:P/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N

Description

D-Link AC2600(DIR-2640) stores the device system account password in plain text. It does not use linux user management. In addition, the passwords of all devices are the same, and they cannot be modified by normal users. An attacker can easily log in to the target router through the serial port and obtain root privileges.

rootfs in firmware

```
$ cat ./etc/shadow
root:$1$ZVpxbK71$2Fgpdj.x9SBOCz5oyULHd/:17349:0:99999:7:::
daemon:*:0:0:99999:7:::
ftp:*:0:0:99999:7:::
network:*:0:0:99999:7:::
nobody:*:0:0:99999:7:::
```

The password of Linux system is `root`

```
$ openssl passwd -1 -salt ZVpxbK71 "root"
$1$ZVpxbK71$2Fgpdj.x9SBOCz5oyULHd/
```

Howerer, we can't log in to the router's console with this password

```
dlinkrouter login: root
Password: [   91.516000] firmadyne: ioctl: 0x41
[   91.536000] firmadyne: ioctl: 0x41

[   96.600000] firmadyne: ioctl: 0x41
[   96.616000] firmadyne: ioctl: 0x41
Login incorrect
```

The script `/sbin/storage.sh` will write a new username and password to `/etc/passwd`

```
admID=`nvram_get 2860 Login`
admPW=`nvram_get 2860 Password`
echo "$admID::0:0:Adminstrator:/:/bin/sh" > /etc/passwd
echo "$admID:x:0:$admID" > /etc/group
```

User name and password are stored in `RT2860_default_vlan`

```
$ cat ./etc_ro/Wireless/RT2860AP/RT2860_default_vlan
...
Login=xxxxx
Password=xxxxxx
...
```

Disclosure Timeline

- 8-Feb-2021 Discoverd the vulnerability
- 9-Feb-2021 Responsibly disclosed vulnerability to vendor
- 10-Feb-2021 D-Link PSIRT would raise to R&D
- 31-Mar-2021 D-Link R&D was investigating the report
- 2-Jun-2021 Requested for CVE-ID assignment
- 10-Jun-2021 CVE-ID Assigned
- 13-Jun-2021 Notified CVE about a publication