

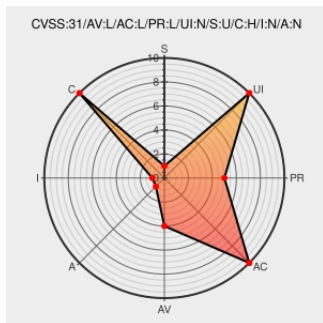


# CVE-2019-14334

Published on: 08/01/2019 12:00:00 AM UTC

Last Modified on: 04/23/2021 05:58:00 PM UTC

## CVE-2019-14334

[Source: Mitre](#)[Source: NIST](#)[CVE.ORG](#)[Print: PDF](#) 

Certain versions of **6600-ap** from **Dlink** contain the following vulnerability:

An issue was discovered on D-Link 6600-AP, DWL-3600AP, and DWL-8610AP Ax 4.2.0.14 21/03/2019 devices. There is post-authenticated Certificate and RSA Private Key extraction through an insecure sslcert-get.cgi HTTP command.

CVE-2019-14334 has been assigned by [M](#) cve@mitre.org to track the vulnerability - currently rated as **MEDIUM** severity.

CVSS3 Score: **5.5 - MEDIUM**

| Attack Vector    | Attack Complexity      | Privileges Required | User Interaction    |
|------------------|------------------------|---------------------|---------------------|
| <b>LOCAL</b>     | <b>LOW</b>             | <b>LOW</b>          | <b>NONE</b>         |
| Scope            | Confidentiality Impact | Integrity Impact    | Availability Impact |
| <b>UNCHANGED</b> | <b>HIGH</b>            | <b>NONE</b>         | <b>NONE</b>         |

CVSS2 Score: **2.1 - LOW**

| Access Vector          | Access Complexity | Authentication      |
|------------------------|-------------------|---------------------|
| <b>LOCAL</b>           | <b>LOW</b>        | <b>NONE</b>         |
| Confidentiality Impact | Integrity Impact  | Availability Impact |
| <b>PARTIAL</b>         | <b>NONE</b>       | <b>NONE</b>         |

## CVE References

| Description                | Tags                                                                                                                                                          | Link                                                     |
|----------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------|
| Security Advisory   D-Link | <a href="#">Vendor Advisory</a><br><a href="#">web.archive.org</a><br><a href="#">text/html</a><br><a href="#">Inactive Link</a> <a href="#">Not Archived</a> | <a href="#">D MISC us.dlink.com/en/security-advisory</a> |

There are currently no QIDs associated with this CVE

| Type                                                                                         | Vendor                | Product                             | Version  | Update | Edition | Language |
|----------------------------------------------------------------------------------------------|-----------------------|-------------------------------------|----------|--------|---------|----------|
| Hardware    | <a href="#">Dlink</a> | <a href="#">6600-ap</a>             | -        | All    | All     | All      |
| Hardware    | <a href="#">Dlink</a> | <a href="#">6600-ap</a>             | -        | All    | All     | All      |
| Operating System                                                                             | <a href="#">Dlink</a> | <a href="#">6600-ap Firmware</a>    | 4.2.0.14 | All    | All     | All      |
| Operating System                                                                             | <a href="#">Dlink</a> | <a href="#">6600-ap Firmware</a>    | 4.2.0.14 | All    | All     | All      |
| Hardware   | <a href="#">Dlink</a> | <a href="#">Dwl-3600ap</a>          | -        | All    | All     | All      |
| Hardware  | <a href="#">Dlink</a> | <a href="#">Dwl-3600ap</a>          | -        | All    | All     | All      |
| Operating System                                                                             | <a href="#">Dlink</a> | <a href="#">Dwl-3600ap Firmware</a> | 4.2.0.14 | All    | All     | All      |
| Operating System                                                                             | <a href="#">Dlink</a> | <a href="#">Dwl-3600ap Firmware</a> | 4.2.0.14 | All    | All     | All      |
| Hardware  | <a href="#">Dlink</a> | <a href="#">Dwl-8610ap</a>          | -        | All    | All     | All      |
| Hardware  | <a href="#">Dlink</a> | <a href="#">Dwl-8610ap</a>          | -        | All    | All     | All      |
| Operating System                                                                             | <a href="#">Dlink</a> | <a href="#">Dwl-8610ap Firmware</a> | 4.2.0.14 | All    | All     | All      |
| Operating System                                                                             | <a href="#">Dlink</a> | <a href="#">Dwl-8610ap Firmware</a> | 4.2.0.14 | All    | All     | All      |

```
cpe:2.3:h:dlink:dwl-3600ap:-:*:*:*:*:*:
```

|                                                     |
|-----------------------------------------------------|
| cpe:2.3:h:dlink:dwl-3600ap:-:*****:                 |
| cpe:2.3:o:dlink:dwl-3600ap_firmware:4.2.0.14:*****: |
| cpe:2.3:o:dlink:dwl-3600ap_firmware:4.2.0.14:*****: |
| cpe:2.3:h:dlink:dwl-8610ap:-:*****:                 |
| cpe:2.3:h:dlink:dwl-8610ap:-:*****:                 |
| cpe:2.3:o:dlink:dwl-8610ap_firmware:4.2.0.14:*****: |
| cpe:2.3:o:dlink:dwl-8610ap_firmware:4.2.0.14:*****: |

No vendor comments have been submitted for this CVE

[← Previous ID](#)

[Next ID →](#)