



Refine search by products

Refine search by vulnerabilities

Search

## Vulnerabilities related to dlink - dir-615

### [CVE-2019-17353](#) (GCVE-0-2019-17353)

Vulnerability from [cvelistv5](#)

#### Published

2019-10-09 11:55

#### Modified

2024-08-05 01:40

#### Severity ?

#### CWE

n/a

#### Summary

An issue discovered on D-Link DIR-615 devices with firmware version 20.05 and 20.07. wan.htm can be accessed directly without authentication, which can lead to disclosure of information about the WAN, and can also be leveraged by an attacker to modify the data fields of the page.

#### References

▼ URL

Tags

#### Impacted products

Vendor

Product

Version

[n/a](#)

[n/a](#)

Version: n/a

[Show details on NVD website](#)

JSON

Share

To clipboard

[Contributors](#) [Documentation](#) [API](#) [About](#)



Vulnerability from [cvelistv5](#)

**Published**

2017-07-07 12:00

**Modified**

2024-08-05 16:04

**Severity ?**

**CWE**

n/a

**Summary**

On the D-Link DIR-615 before v20.12PTb04, if a victim logged in to the Router's Web Interface visits a malicious site from another Browser tab, the malicious site then can send requests to the victim's Router without knowing the credentials (CSRF). An attacker can host a page that sends a POST request to Form2File.htm that tries to upload Firmware to victim's Router. This causes the router to reboot/crash resulting in Denial of Service. An attacker may succeed in uploading malicious Firmware.

**References**

▼ URL

Tags

**Impacted products**

**Vendor**

**Product**

**Version**

[n/a](#)

[n/a](#)

**Version:** n/a

[Show details on NVD website](#)

JSON

Share

To clipboard

[CVE-2019-19742](#) (GCVE-0-2019-19742)

Vulnerability from [cvelistv5](#)

**Published**

2019-12-18 12:19

**Modified**

2024-08-05 02:25

**Severity ?**

**CWE**

n/a

**Summary**

On D-Link DIR-615 devices, the User Account Configuration page is



vulnerable to blind XSS via the name field.

References

▼ URL

Tags

Impacted products

Vendor

Product

Version

[n/a](#)

[n/a](#)

Version: n/a

[Show details on NVD website](#)

JSON

Share

To clipboard

[CVE-2009-4821](#) (GCVE-0-2009-4821)

Vulnerability from [cvelistv5](#)

Published

2010-04-27 15:00

Modified

2024-09-17 01:36

Severity ?

CWE

n/a

Summary

The D-Link DIR-615 with firmware 3.10NA does not require administrative authentication for apply.cgi, which allows remote attackers to (1) change the admin password via the admin\_password parameter, (2) disable the security requirement for the Wi-Fi network via unspecified vectors, or (3) modify DNS settings via unspecified vectors.

References

▼ URL

Tags

Impacted products

Vendor

Product

Version

[n/a](#)

[n/a](#)

Version: n/a

[Show details on NVD website](#)



JSON

Share

To clipboard

[CVE-2017-7405](#) (GCVE-0-2017-7405)

Vulnerability from [cvelistv5](#)

**Published**

2017-07-07 12:00

**Modified**

2024-08-05 16:04

**Severity ?**

**CWE**

n/a

**Summary**

On the D-Link DIR-615 before v20.12PTb04, once authenticated, this device identifies the user based on the IP address of his machine. By spoofing the IP address belonging to the victim's host, an attacker might be able to take over the administrative session without being prompted for authentication credentials. An attacker can get the victim's and router's IP addresses by simply sniffing the network traffic. Moreover, if the victim has web access enabled on his router and is accessing the web interface from a different network that is behind the NAT/Proxy, an attacker can sniff the network traffic to know the public IP address of the victim's router and take over his session as he won't be prompted for credentials.

**References**

▼ URL

Tags

**Impacted products**

Vendor	Product	Version
<a href="#">n/a</a>	<a href="#">n/a</a>	<b>Version:</b> n/a

[Show details on NVD website](#)

JSON

Share

To clipboard

[CVE-2024-0717](#) (GCVE-0-2024-0717)

Vulnerability from [cvelistv5](#)

**Published**

2024-01-19 15:31



Modified

2025-05-30 14:26

Severity ?

5.3 (Medium) - [CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N](#)

5.3 (Medium) - [CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N](#)

CWE

[CWE-200](#) - Information Disclosure

Summary


A vulnerability classified as critical was found in D-Link DAP-1360, DIR-300, DIR-615, DIR-615GF, DIR-615S, DIR-615T, DIR-620, DIR-620S, DIR-806A, DIR-815, DIR-815AC, DIR-815S, DIR-816, DIR-820, DIR-822, DIR-825, DIR-825AC, DIR-825ACF, DIR-825ACG1, DIR-841, DIR-842, DIR-842S, DIR-843, DIR-853, DIR-878, DIR-882, DIR-1210, DIR-1260, DIR-2150, DIR-X1530, DIR-X1860, DSL-224, DSL-245GR, DSL-2640U, DSL-2750U, DSL-G2452GR, DVG-5402G, DVG-5402G, DVG-5402GFRU, DVG-N5402G, DVG-N5402G-IL, DWM-312W, DWM-321, DWR-921, DWR-953 and Good Line Router v2 up to 20240112. This vulnerability affects unknown code of the file /devinfo of the component HTTP GET Request Handler. The manipulation of the argument area with the input notice|net|version leads to information disclosure. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used. VDB-251542 is the identifier assigned to this vulnerability.

References

▼ URL

Tags

Impacted products

Vendor	Product	Version	
▼ <a href="#">D-Link</a>	<a href="#">DAP-1360</a>	Version: 20240112	

[Show details on NVD website](#)

JSON

Share

To clipboard

[CVE-2018-10431](#) (GCVE-0-2018-10431)

Vulnerability from [cvelistv5](#)

Published

2018-04-26 17:00



Modified

2024-08-05 07:39

Severity ?

CWE

n/a

Summary

D-Link DIR-615 2.5.17 devices allow Remote Code Execution via shell metacharacters in the Host field of the System / Traceroute screen.

References

▼ URL

Tags

Impacted products

Vendor

Product

Version

[n/a](#)

[n/a](#)

Version: n/a

[Show details on NVD website](#)

JSON

Share

To clipboard

[CVE-2018-25115](#) (GCVE-0-2018-25115)

Vulnerability from [cvelistv5](#)

Published

2025-08-27 21:24

Modified

2025-08-28 19:45

Severity ?

10.0 (Critical) - [CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:N/VC:H/VI:H/VA:H/SC:H/SI:H/SA:H](#)

CWE

[CWE-78](#) - Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')

Summary

Multiple D-Link DIR-series routers, including DIR-110, DIR-412, DIR-600, DIR-610, DIR-615, DIR-645, and DIR-815 firmware version 1.03, contain a vulnerability in the service.cgi endpoint that allows remote attackers to execute arbitrary system commands without authentication. The flaw stems from improper input handling in the EVENT=CHECKFW parameter, which is passed directly to the




system shell without sanitization. A crafted HTTP POST request can inject commands that are executed with root privileges, resulting in full device compromise. These router models are no longer supported at the time of assignment and affected version ranges may vary. Exploitation evidence was first observed by the Shadowserver Foundation on 2025-08-21 UTC.

References

▼ URL

Tags

Impacted products

Vendor	Product	Version
▼ <a href="#">D-Link</a>	<a href="#">DIR-110</a>	Version: * 

[Show details on NVD website](#)

JSON

Share

To clipboard

[CVE-2019-17525](#) (GCVE-0-2019-17525)

Vulnerability from [cvelistv5](#)

Published

2020-04-21 18:57

Modified

2024-08-05 01:40

Severity ?

CWE

n/a

Summary

The login page on D-Link DIR-615 T1 20.10 devices allows remote attackers to bypass the CAPTCHA protection mechanism and conduct brute-force attacks.

References

▼ URL

Tags

Impacted products

Vendor	Product	Version
<a href="#">n/a</a>	<a href="#">n/a</a>	Version: n/a

[Show details on NVD website](#)



JSON

Share

To clipboard

[CVE-2017-11436](#) (GCVE-0-2017-11436)

Vulnerability from [cvelistv5](#)

**Published**

2017-07-19 07:00

**Modified**

2024-08-05 18:12

**Severity ?**

**CWE**

n/a

**Summary**

D-Link DIR-615 before v20.12PTb04 has a second admin account with a 0x1 BACKDOOR value, which might allow remote attackers to obtain access via a TELNET connection.

**References**

▼ URL

Tags

**Impacted products**

Vendor	Product	Version
<a href="#">n/a</a>	<a href="#">n/a</a>	<b>Version:</b> n/a

[Show details on NVD website](#)

JSON

Share

To clipboard

[CVE-2021-40654](#) (GCVE-0-2021-40654)

Vulnerability from [cvelistv5](#)

**Published**

2021-09-24 20:02

**Modified**

2024-08-04 02:51

**Severity ?**

**CWE**

n/a

**Summary**

An information disclosure issue exist in D-LINK-DIR-615 B2 2.01mt.





An attacker can obtain a user name and password by forging a post request to the / getcfg.php page

References

▼ URL

Tags

Impacted products

Vendor

Product

Version

[n/a](#)

[n/a](#)

Version: n/a

[Show details on NVD website](#)

JSON

Share

To clipboard

[CVE-2018-15874](#) (GCVE-0-2018-15874)

Vulnerability from [cvelistv5](#)

Published

2018-08-25 19:00

Modified

2024-08-05 10:10

Severity ?

CWE

n/a

Summary

Cross-site scripting (XSS) vulnerability on D-Link DIR-615 routers 20.07 allows an attacker to inject JavaScript into the "Status -> Active Client Table" page via the hostname field in a DHCP request.

References

▼ URL

Tags

Impacted products

Vendor

Product

Version

[n/a](#)

[n/a](#)

Version: n/a

[Show details on NVD website](#)

JSON

Share

To clipboard



[CVE-2013-10050](#) (GCVE-0-2013-10050)

Vulnerability from [cvelistv5](#)

**Published**

2025-08-01 20:39

**Modified**

2025-08-04 14:23

**Severity ?**

8.7 (High) - [CVSS:4.0/AV:N/AC:L/AT:N/PR:L/UI:N/VC:H/VI:H/VA:H/SC:N/SI:N/SA:N](#)

**CWE**

[CWE-78](#) - Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')

**Summary**

An OS command injection vulnerability exists in multiple D-Link routers—confirmed on DIR-300 rev A (v1.05) and DIR-615 rev D (v4.13)—via the authenticated tools\_vct.xgi CGI endpoint. The web interface fails to properly sanitize user-supplied input in the pingIp parameter, allowing attackers with valid credentials to inject arbitrary shell commands. Exploitation enables full device compromise, including spawning a telnet daemon and establishing a root shell. The vulnerability is present in firmware versions that expose tools\_vct.xgi and use the Mathopd/1.5p6 web server. No vendor patch is available, and affected models are end-of-life.

**References**

▼ URL

Tags

**Impacted products**

Vendor	Product	Version
▼ <a href="#">D-Link</a>	<a href="#">DIR-300 rev A</a>	<b>Version: *</b> ≤ 1.05 

[Show details on NVD website](#)

JSON

Share

To clipboard

[CVE-2014-8361](#) (GCVE-0-2014-8361)

Vulnerability from [cvelistv5](#)

**Published**

2015-05-01 00:00



Modified

2025-07-30 01:46

Severity ?

9.8 (Critical) - [CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H](#)

CWE

n/a

Summary

The miniigd SOAP service in Realtek SDK allows remote attackers to execute arbitrary code via a crafted NewInternalClient request, as exploited in the wild through 2023.

References

▼ URL

Tags

Impacted products

Vendor

Product

Version

[n/a](#)

[n/a](#)

Version: n/a

[Show details on NVD website](#)

JSON

Share

To clipboard

[CVE-2018-15875](#) (GCVE-0-2018-15875)

Vulnerability from [cvelistv5](#)

Published

2018-08-25 19:00

Modified

2024-08-05 10:10

Severity ?

CWE

n/a

Summary

Cross-site scripting (XSS) vulnerability on D-Link DIR-615 routers 20.07 allows attackers to inject JavaScript into the router's admin UPnP page via the description field in an AddPortMapping UPnP SOAP request.

References

▼ URL

Tags

Impacted products



Vendor	Product	Version
<a href="#">n/a</a>	<a href="#">n/a</a>	<b>Version:</b> n/a

[Show details on NVD website](#)

JSON

Share

To clipboard

[CVE-2017-7398](#) (GCVE-0-2017-7398)  
Vulnerability from [cvelistv5](#)

**Published**  
2017-04-04 14:00

**Modified**  
2024-08-05 16:04

**Severity ?**

**CWE**  
n/a

**Summary**  
D-Link DIR-615 HW: T1 FW:20.09 is vulnerable to Cross-Site Request Forgery (CSRF) vulnerability. This enables an attacker to perform an unwanted action on a wireless router for which the user/admin is currently authenticated, as demonstrated by changing the Security option from WPA2 to None, or changing the hiddenSSID parameter, SSID parameter, or a security-option password.

**References**

▼ URL

Tags

**Impacted products**

Vendor	Product	Version
<a href="#">n/a</a>	<a href="#">n/a</a>	<b>Version:</b> n/a

[Show details on NVD website](#)

JSON

Share

To clipboard

[CVE-2017-9542](#) (GCVE-0-2017-9542)  
Vulnerability from [cvelistv5](#)

**Published**



2017-06-11 23:00

Modified

2024-08-05 17:11

Severity ?

CWE

n/a

Summary

D-Link DIR-615 Wireless N 300 Router allows authentication bypass via a modified POST request to login.cgi. This issue occurs because it fails to validate the password field. Successful exploitation of this issue allows an attacker to take control of the affected device.

References

▼ URL

Tags

Impacted products

Vendor

Product

Version

[n/a](#)

[n/a](#)

Version: n/a

[Show details on NVD website](#)

JSON

Share

To clipboard

[CVE-2021-42627](#) (GCVE-0-2021-42627)

Vulnerability from [cvelistv5](#)

Published

2022-08-23 11:51

Modified

2024-08-04 03:38

Severity ?

CWE

n/a

Summary

The WAN configuration page "wan.htm" on D-Link DIR-615 devices with firmware 20.06 can be accessed directly without authentication which can lead to disclose the information about WAN settings and also leverage attacker to modify the data fields of page.

References

▼ URL

Tags



Impacted products

Vendor	Product	Version
<a href="#">n/a</a>	<a href="#">n/a</a>	<b>Version:</b> n/a

[Show details on NVD website](#)

JSON

Share

To clipboard

[CVE-2017-7406](#) (GCVE-0-2017-7406)

Vulnerability from [cvelistv5](#)

Published

2017-07-07 12:00

Modified

2024-08-05 16:04

Severity ?

CWE

n/a

Summary

The D-Link DIR-615 device before v20.12PTb04 doesn't use SSL for any of the authenticated pages. Also, it doesn't allow the user to generate his own SSL Certificate. An attacker can simply monitor network traffic to steal a user's credentials and/or credentials of users being added while sniffing the traffic.

References

▼ URL

Tags

Impacted products

Vendor	Product	Version
<a href="#">n/a</a>	<a href="#">n/a</a>	<b>Version:</b> n/a

[Show details on NVD website](#)

JSON

Share

To clipboard

[CVE-2021-37388](#) (GCVE-0-2021-37388)

Vulnerability from [cvelistv5](#)



Published

2021-08-06 11:22

Modified

2024-08-04 01:16

Severity ?

CWE

n/a

Summary

A buffer overflow in D-Link DIR-615 C2 3.03WW. The ping\_ipaddr parameter in ping\_response.cgi POST request allows an attacker to crash the webserver and might even gain remote code execution.

References

▼ URL

Tags

Impacted products

Vendor

Product

Version

[n/a](#)

[n/a](#)

Version: n/a

[Show details on NVD website](#)

JSON

Share

To clipboard

[CVE-2019-16920](#) (GCVE-0-2019-16920)

Vulnerability from [cvelistv5](#)

Published

2019-09-27 11:34

Modified

2025-07-30 01:45

Severity ?

9.8 (Critical) - [CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H](#)

CWE

n/a

Summary

Unauthenticated remote code execution occurs in D-Link products such as DIR-655C, DIR-866L, DIR-652, and DHP-1565. The issue occurs when the attacker sends an arbitrary input to a "PingTest" device common gateway interface that could lead to common injection. An attacker who successfully triggers the command injection could achieve full system compromise. Later, it was



independently found that these are also affected: DIR-855L, DAP-1533, DIR-862L, DIR-615, DIR-835, and DIR-825.

References

▼ URL

Tags

Impacted products

Vendor	Product	Version
<a href="#">n/a</a>	<a href="#">n/a</a>	Version: n/a

[Show details on NVD website](#)

JSON

Share

To clipboard

[CVE-2018-15839](#) (GCVE-0-2018-15839)

Vulnerability from [cvelistv5](#)

Published

2018-08-28 17:00

Modified

2024-08-05 10:01

Severity ?

CWE

n/a

Summary

D-Link DIR-615 devices have a buffer overflow via a long Authorization HTTP header.

References

▼ URL

Tags

Impacted products

Vendor	Product	Version
<a href="#">n/a</a>	<a href="#">n/a</a>	Version: n/a

[Show details on NVD website](#)

JSON

Share

To clipboard

Vulnerability from [fkie\\_nvd](#)





**Published**

2017-07-07 12:29

**Modified**

2025-04-20 01:37

**Severity ?**

9.8 (Critical) - [CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H](#)

**Summary**

On the D-Link DIR-615 before v20.12PTb04, once authenticated, this device identifies the user based on the IP address of his machine. By spoofing the IP address belonging to the victim's host, an attacker might be able to take over the administrative session without being prompted for authentication credentials. An attacker can get the victim's and router's IP addresses by simply sniffing the network traffic. Moreover, if the victim has web access enabled on his router and is accessing the web interface from a different network that is behind the NAT/Proxy, an attacker can sniff the network traffic to know the public IP address of the victim's router and take over his session as he won't be prompted for credentials.

**References**

▼ URL

Tags

**Impacted products**

Vendor	Product	Version
<a href="#">dlink</a>	<a href="#">dir-615</a>	*
<a href="#">dlink</a>	<a href="#">dir-615</a>	*

JSON

Share

To clipboard

Vulnerability from [fkie\\_nvd](#)

**Published**

2017-04-04 14:59

**Modified**

2025-04-20 01:37

**Severity ?**

8.8 (High) - [CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H](#)

**Summary**

D-Link DIR-615 HW: T1 FW:20.09 is vulnerable to Cross-Site



Request Forgery (CSRF) vulnerability. This enables an attacker to perform an unwanted action on a wireless router for which the user/admin is currently authenticated, as demonstrated by changing the Security option from WPA2 to None, or changing the hiddenSSID parameter, SSID parameter, or a security-option password.

References

▼ URL

Tags

Impacted products

Vendor	Product	Version
<a href="#">d-link</a>	<a href="#">dir-615_firmware</a>	20.09
<a href="#">dlink</a>	<a href="#">dir-615</a>	-

JSON

Share

To clipboard

Vulnerability from [fkie\\_nvd](#)

Published

2018-08-25 19:29

Modified

2024-11-21 03:51

Severity ?

6.1 (Medium) - [CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:C/C:L/I:L/A:N](#)

Summary

Cross-site scripting (XSS) vulnerability on D-Link DIR-615 routers 20.07 allows an attacker to inject JavaScript into the "Status -> Active Client Table" page via the hostname field in a DHCP request.

References

▼ URL

Tags

Impacted products

Vendor	Product	Version
<a href="#">dlink</a>	<a href="#">dir-615_firmware</a>	20.07
<a href="#">dlink</a>	<a href="#">dir-615</a>	t1



JSON

Share

To clipboard

Vulnerability from [fkie\\_nvd](#)

**Published**

2021-08-06 12:15

**Modified**

2024-11-21 06:15

**Severity ?**

9.8 (Critical) - [CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H](#)

**Summary**

A buffer overflow in D-Link DIR-615 C2 3.03WW. The ping\_ipaddr parameter in ping\_response.cgi POST request allows an attacker to crash the webserver and might even gain remote code execution.

**References**

▼ URL

Tags

**Impacted products**

Vendor	Product	Version
<a href="#">dlink</a>	<a href="#">dir-615_firmware</a>	3.03ww
<a href="#">dlink</a>	<a href="#">dir-615</a>	c2

JSON

Share

To clipboard

Vulnerability from [fkie\\_nvd](#)

**Published**

2021-09-24 21:15

**Modified**

2024-11-21 06:24

**Severity ?**

6.5 (Medium) - [CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N](#)

**Summary**

An information disclosure issue exist in D-LINK-DIR-615 B2 2.01mt. An attacker can obtain a user name and password by forging a post request to the / getcfg.php page



References

▼ URL

Tags

Impacted products

Vendor	Product	Version
<a href="#">dlink</a>	<a href="#">dir-615_firmware</a>	17.00
<a href="#">dlink</a>	<a href="#">dir-615</a>	q1

JSON

Share

To clipboard

Vulnerability from [fkie\\_nvd](#)

Published

2019-10-09 12:15

Modified

2024-11-21 04:32

Severity ?

8.2 (High) - [CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:H/A:N](#)

Summary

An issue discovered on D-Link DIR-615 devices with firmware version 20.05 and 20.07. wan.htm can be accessed directly without authentication, which can lead to disclosure of information about the WAN, and can also be leveraged by an attacker to modify the data fields of the page.

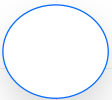
References

▼ URL

Tags

Impacted products

Vendor	Product	Version
<a href="#">dlink</a>	<a href="#">dir-615_firmware</a>	20.05
<a href="#">dlink</a>	<a href="#">dir-615_firmware</a>	20.07
<a href="#">dlink</a>	<a href="#">dir-615</a>	-



JSON

Share

To clipboard

Vulnerability from [fkie\\_nvd](#)

**Published**

2024-01-19 16:15

**Modified**

2024-11-21 08:47

**Severity ?**

5.3 (Medium) - [CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N](#)

5.3 (Medium) - [CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N](#)

**Summary**

A vulnerability classified as critical was found in D-Link DAP-1360, DIR-300, DIR-615, DIR-615GF, DIR-615S, DIR-615T, DIR-620, DIR-620S, DIR-806A, DIR-815, DIR-815AC, DIR-815S, DIR-816, DIR-820, DIR-822, DIR-825, DIR-825AC, DIR-825ACF, DIR-825ACG1, DIR-841, DIR-842, DIR-842S, DIR-843, DIR-853, DIR-878, DIR-882, DIR-1210, DIR-1260, DIR-2150, DIR-X1530, DIR-X1860, DSL-224, DSL-245GR, DSL-2640U, DSL-2750U, DSL-G2452GR, DVG-5402G, DVG-5402G, DVG-5402GFRU, DVG-N5402G, DVG-N5402G-IL, DWM-312W, DWM-321, DWR-921, DWR-953 and Good Line Router v2 up to 20240112. This vulnerability affects unknown code of the file /devinfo of the component HTTP GET Request Handler. The manipulation of the argument area with the input notice|net|version leads to information disclosure. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used. VDB-251542 is the identifier assigned to this vulnerability.

**References**

▼ URL

Tags

**Impacted products**

Vendor	Product	Version
<a href="#">dlink</a>	<a href="#">dir-825acg1_firmware</a>	*
<a href="#">dlink</a>	<a href="#">dir-825acg1</a>	-
<a href="#">dlink</a>	<a href="#">dir-841_firmware</a>	*
<a href="#">dlink</a>	<a href="#">dir-841</a>	-



Vendor	Product	Version
<a href="#">dlink</a>	<a href="#">dir-1260_firmware</a>	*
<a href="#">dlink</a>	<a href="#">dir-1260</a>	-
<a href="#">dlink</a>	<a href="#">dir-822_firmware</a>	*
<a href="#">dlink</a>	<a href="#">dir-822</a>	-
<a href="#">dlink</a>	<a href="#">dir-x1530_firmware</a>	*
<a href="#">dlink</a>	<a href="#">dir-x1530</a>	-
<a href="#">dlink</a>	<a href="#">dir-825_firmware</a>	*
<a href="#">dlink</a>	<a href="#">dir-825</a>	-
<a href="#">dlink</a>	<a href="#">dir-615_firmware</a>	*
<a href="#">dlink</a>	<a href="#">dir-615</a>	-
<a href="#">dlink</a>	<a href="#">dir-842_firmware</a>	*
<a href="#">dlink</a>	<a href="#">dir-842</a>	-
<a href="#">dlink</a>	<a href="#">dir-853_firmware</a>	*
<a href="#">dlink</a>	<a href="#">dir-853</a>	-
<a href="#">dlink</a>	<a href="#">dir-1210_firmware</a>	*
<a href="#">dlink</a>	<a href="#">dir-1210</a>	-
<a href="#">dlink</a>	<a href="#">dir-806a_firmware</a>	*
<a href="#">dlink</a>	<a href="#">dir-806a</a>	-
<a href="#">dlink</a>	<a href="#">dir-815_firmware</a>	*
<a href="#">dlink</a>	<a href="#">dir-815</a>	-
<a href="#">dlink</a>	<a href="#">dsl-245gr_firmware</a>	*
<a href="#">dlink</a>	<a href="#">dsl-245gr</a>	-
<a href="#">dlink</a>	<a href="#">dsl-g2452gr_firmware</a>	*
<a href="#">dlink</a>	<a href="#">dsl-g2452gr</a>	-



Vendor	Product	Version
<a href="#">dlink</a>	<a href="#">dir-878_firmware</a>	*
<a href="#">dlink</a>	<a href="#">dir-878</a>	-
<a href="#">dlink</a>	<a href="#">dir-825acf_firmware</a>	*
<a href="#">dlink</a>	<a href="#">dir-825acf</a>	-
<a href="#">dlink</a>	<a href="#">dir-615t_firmware</a>	*
<a href="#">dlink</a>	<a href="#">dir-615t</a>	-
<a href="#">dlink</a>	<a href="#">dir-300_firmware</a>	*
<a href="#">dlink</a>	<a href="#">dir-300</a>	-
<a href="#">dlink</a>	<a href="#">dir-842s_firmware</a>	*
<a href="#">dlink</a>	<a href="#">dir-842s</a>	-
<a href="#">dlink</a>	<a href="#">dir-815s_firmware</a>	*
<a href="#">dlink</a>	<a href="#">dir-815s</a>	-
<a href="#">dlink</a>	<a href="#">dsl-2640u_firmware</a>	*
<a href="#">dlink</a>	<a href="#">dsl-2640u</a>	-
<a href="#">dlink</a>	<a href="#">dir-2150_firmware</a>	*
<a href="#">dlink</a>	<a href="#">dir-2150</a>	-
<a href="#">dlink</a>	<a href="#">dwr-921_firmware</a>	*
<a href="#">dlink</a>	<a href="#">dwr-921</a>	-
<a href="#">dlink</a>	<a href="#">dir-615s_firmware</a>	*
<a href="#">dlink</a>	<a href="#">dir-615s</a>	-
<a href="#">dlink</a>	<a href="#">dir-620_firmware</a>	*
<a href="#">dlink</a>	<a href="#">dir-620</a>	-
<a href="#">dlink</a>	<a href="#">dvg-5402g_firmware</a>	*
<a href="#">dlink</a>	<a href="#">dvg-5402g</a>	-



Vendor	Product	Version
<a href="#">dlink</a>	<a href="#">dir-882_firmware</a>	*
<a href="#">dlink</a>	<a href="#">dir-882</a>	-
<a href="#">dlink</a>	<a href="#">dwm-312w_firmware</a>	*
<a href="#">dlink</a>	<a href="#">dwm-312w</a>	-
<a href="#">dlink</a>	<a href="#">dir-815\ac_firmware</a>	*
<a href="#">dlink</a>	<a href="#">dir-815\ac</a>	-
<a href="#">dlink</a>	<a href="#">dsl-224_firmware</a>	*
<a href="#">dlink</a>	<a href="#">dsl-224</a>	-
<a href="#">dlink</a>	<a href="#">dwm-321_firmware</a>	*
<a href="#">dlink</a>	<a href="#">dwm-321</a>	-
<a href="#">dlink</a>	<a href="#">dir-x1860_firmware</a>	*
<a href="#">dlink</a>	<a href="#">dir-x1860</a>	-
<a href="#">dlink</a>	<a href="#">dap-1360_firmware</a>	*
<a href="#">dlink</a>	<a href="#">dap-1360</a>	-
<a href="#">dlink</a>	<a href="#">dir-820_firmware</a>	*
<a href="#">dlink</a>	<a href="#">dir-820</a>	-
<a href="#">dlink</a>	<a href="#">dir-843_firmware</a>	*
<a href="#">dlink</a>	<a href="#">dir-843</a>	-
<a href="#">dlink</a>	<a href="#">dvg-5402g\gfru_firmware</a>	*
<a href="#">dlink</a>	<a href="#">dvg-5402g\gfru</a>	-
<a href="#">dlink</a>	<a href="#">dwr-953_firmware</a>	*
<a href="#">dlink</a>	<a href="#">dwr-953</a>	-
<a href="#">dlink</a>	<a href="#">dvg-n5402g\il_firmware</a>	*
<a href="#">dlink</a>	<a href="#">dvg-n5402g\il</a>	-





Vendor	Product	Version
<a href="#">dlink</a>	<a href="#">dir-825ac_firmware</a>	*
<a href="#">dlink</a>	<a href="#">dir-825ac</a>	-
<a href="#">dlink</a>	<a href="#">dir-620s_firmware</a>	*
<a href="#">dlink</a>	<a href="#">dir-620s</a>	-
<a href="#">dlink</a>	<a href="#">dvg-n5402g_firmware</a>	*
<a href="#">dlink</a>	<a href="#">dvg-n5402g</a>	-
<a href="#">dlink</a>	<a href="#">dsl-2750u_firmware</a>	*
<a href="#">dlink</a>	<a href="#">dsl-2750u</a>	-
<a href="#">dlink</a>	<a href="#">dir-615gf_firmware</a>	*
<a href="#">dlink</a>	<a href="#">dir-615gf</a>	-
<a href="#">dlink</a>	<a href="#">dir-816_firmware</a>	*
<a href="#">dlink</a>	<a href="#">dir-816</a>	-

JSON

Share

To clipboard

Vulnerability from [fkie\\_nvd](#)

**Published**  
2018-04-26 17:29

**Modified**  
2024-11-21 03:41

**Severity ?**  
7.2 (High) - [CVSS:3.0/AV:N/AC:L/PR:H/UI:N/S:U/C:H/I:H/A:H](#)

**Summary**  
D-Link DIR-615 2.5.17 devices allow Remote Code Execution via shell metacharacters in the Host field of the System / Traceroute screen.

**References**

▼ URL

Tags

Impacted products

Vendor	Product	Version
<a href="#">d-link</a>	<a href="#">dir-615_firmware</a>	2.5.17
<a href="#">dlink</a>	<a href="#">dir-615</a>	-

JSON

Share

To clipboard

Vulnerability from [fkie\\_nvd](#)

Published

2018-08-28 17:29

Modified

2024-11-21 03:51

Severity ?

9.8 (Critical) - [CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H](#)

Summary

D-Link DIR-615 devices have a buffer overflow via a long Authorization HTTP header.

References

▼ URL

Tags

Impacted products

Vendor	Product	Version
<a href="#">dlink</a>	<a href="#">dir-615_firmware</a>	-
<a href="#">dlink</a>	<a href="#">dir-615</a>	-

JSON

Share

To clipboard

Vulnerability from [fkie\\_nvd](#)

Published

2025-08-27 22:15

Modified



2025-09-24 18:03

Severity ?

9.8 (Critical) - [CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H](#)

Summary

Multiple D-Link DIR-series routers, including DIR-110, DIR-412, DIR-600, DIR-610, DIR-615, DIR-645, and DIR-815 firmware version 1.03, contain a vulnerability in the service.cgi endpoint that allows remote attackers to execute arbitrary system commands without authentication. The flaw stems from improper input handling in the EVENT=CHECKFW parameter, which is passed directly to the system shell without sanitization. A crafted HTTP POST request can inject commands that are executed with root privileges, resulting in full device compromise. These router models are no longer supported at the time of assignment and affected version ranges may vary. Exploitation evidence was first observed by the Shadowserver Foundation on 2025-08-21 UTC.

References

▼ URL

Tags

Impacted products

Vendor	Product	Version
<a href="#">dlink</a>	<a href="#">dir-110_firmware</a>	-
<a href="#">dlink</a>	<a href="#">dir-110</a>	-
<a href="#">dlink</a>	<a href="#">dir-412_firmware</a>	-
<a href="#">dlink</a>	<a href="#">dir-412</a>	-
<a href="#">dlink</a>	<a href="#">dir-600_firmware</a>	-
<a href="#">dlink</a>	<a href="#">dir-600</a>	-
<a href="#">dlink</a>	<a href="#">dir-610_firmware</a>	-
<a href="#">dlink</a>	<a href="#">dir-610</a>	-
<a href="#">dlink</a>	<a href="#">dir-615_firmware</a>	-
<a href="#">dlink</a>	<a href="#">dir-615</a>	-
<a href="#">dlink</a>	<a href="#">dir-645_firmware</a>	-
<a href="#">dlink</a>	<a href="#">dir-645</a>	-



Vendor	Product	Version
<a href="#">dlink</a>	<a href="#">dir-815_firmware</a>	1.03
<a href="#">dlink</a>	<a href="#">dir-815</a>	-

JSON

Share

To clipboard

Vulnerability from [fkie\\_nvd](#)

**Published**  
2018-08-25 19:29

**Modified**  
2024-11-21 03:51

**Severity ?**  
6.1 (Medium) - [CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:C/C:L/I:L/A:N](#)

**Summary**  
Cross-site scripting (XSS) vulnerability on D-Link DIR-615 routers 20.07 allows attackers to inject JavaScript into the router's admin UPnP page via the description field in an AddPortMapping UPnP SOAP request.

**References**

▼ URL

Tags

**Impacted products**

Vendor	Product	Version
<a href="#">dlink</a>	<a href="#">dir-615_firmware</a>	20.07
<a href="#">dlink</a>	<a href="#">dir-615</a>	t1

JSON

Share

To clipboard

Vulnerability from [fkie\\_nvd](#)

**Published**  
2022-08-23 12:15



Modified

2024-11-21 06:27

Severity ?

9.8 (Critical) - [CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H](#)

Summary

The WAN configuration page "wan.htm" on D-Link DIR-615 devices with firmware 20.06 can be accessed directly without authentication which can lead to disclose the information about WAN settings and also leverage attacker to modify the data fields of page.

References

▼ URL

Tags

Impacted products

Vendor	Product	Version
<a href="#">dlink</a>	<a href="#">dir-615_firmware</a>	20.06
<a href="#">dlink</a>	<a href="#">dir-615</a>	-
<a href="#">dlink</a>	<a href="#">dir-615_j1_firmware</a>	20.06
<a href="#">dlink</a>	<a href="#">dir-615_j1</a>	-
<a href="#">dlink</a>	<a href="#">dir-615_t1_firmware</a>	20.06
<a href="#">dlink</a>	<a href="#">dir-615_t1</a>	-
<a href="#">dlink</a>	<a href="#">dir-615jx10_firmware</a>	20.06
<a href="#">dlink</a>	<a href="#">dir-615jx10</a>	-

JSON

Share

To clipboard

Vulnerability from [fkie\\_nvd](#)

Published

2017-07-07 12:29

Modified

2025-04-20 01:37

Severity ?

9.8 (Critical) - [CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H](#)



### Summary

The D-Link DIR-615 device before v20.12PTb04 doesn't use SSL for any of the authenticated pages. Also, it doesn't allow the user to generate his own SSL Certificate. An attacker can simply monitor network traffic to steal a user's credentials and/or credentials of users being added while sniffing the traffic.

### References

▼ URL

Tags

### Impacted products

Vendor	Product	Version
<a href="#">dlink</a>	<a href="#">dir-615</a>	*
<a href="#">dlink</a>	<a href="#">dir-615</a>	*

JSON

Share

To clipboard

Vulnerability from [fkie\\_nvd](#)

### Published

2019-09-27 12:15

### Modified

2025-04-03 19:51

### Severity ?

9.8 (Critical) - [CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H](#)

9.8 (Critical) - [CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H](#)

### Summary

Unauthenticated remote code execution occurs in D-Link products such as DIR-655C, DIR-866L, DIR-652, and DHP-1565. The issue occurs when the attacker sends an arbitrary input to a "PingTest" device common gateway interface that could lead to common injection. An attacker who successfully triggers the command injection could achieve full system compromise. Later, it was independently found that these are also affected: DIR-855L, DAP-1533, DIR-862L, DIR-615, DIR-835, and DIR-825.

### References

▼ URL

Tags



## Impacted products

Vendor	Product	Version
<a href="#">dlink</a>	<a href="#">dir-655_firmware</a>	*
<a href="#">dlink</a>	<a href="#">dir-655</a>	CX
<a href="#">dlink</a>	<a href="#">dir-866L_firmware</a>	*
<a href="#">dlink</a>	<a href="#">dir-866l</a>	ax
<a href="#">dlink</a>	<a href="#">dir-652_firmware</a>	-
<a href="#">dlink</a>	<a href="#">dir-652</a>	ax
<a href="#">dlink</a>	<a href="#">dhp-1565_firmware</a>	*
<a href="#">dlink</a>	<a href="#">dhp-1565</a>	ax
<a href="#">dlink</a>	<a href="#">dir-855L_firmware</a>	-
<a href="#">dlink</a>	<a href="#">dir-855l</a>	-
<a href="#">dlink</a>	<a href="#">dap-1533_firmware</a>	-
<a href="#">dlink</a>	<a href="#">dap-1533</a>	-
<a href="#">dlink</a>	<a href="#">dir-862L_firmware</a>	-
<a href="#">dlink</a>	<a href="#">dir-862l</a>	-
<a href="#">dlink</a>	<a href="#">dir-615_firmware</a>	-
<a href="#">dlink</a>	<a href="#">dir-615</a>	-
<a href="#">dlink</a>	<a href="#">dir-835_firmware</a>	-
<a href="#">dlink</a>	<a href="#">dir-835</a>	-
<a href="#">dlink</a>	<a href="#">dir-825_firmware</a>	-
<a href="#">dlink</a>	<a href="#">dir-825</a>	-

JSON

Share

To clipboard



Vulnerability from [fkie\\_nvd](#)

**Published**

2017-06-11 23:29

**Modified**

2025-04-20 01:37

**Severity ?**

9.8 (Critical) - [CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H](#)

**Summary**

D-Link DIR-615 Wireless N 300 Router allows authentication bypass via a modified POST request to login.cgi. This issue occurs because it fails to validate the password field. Successful exploitation of this issue allows an attacker to take control of the affected device.

**References**

▼ URL

Tags

**Impacted products**

Vendor	Product	Version
<a href="#">d-link</a>	<a href="#">dir-615_firmware</a>	*
<a href="#">dlink</a>	<a href="#">dir-615</a>	-

JSON

Share

To clipboard

Vulnerability from [fkie\\_nvd](#)

**Published**

2010-04-27 15:30

**Modified**

2025-04-11 00:51

**Severity ?**

**Summary**

The D-Link DIR-615 with firmware 3.10NA does not require administrative authentication for apply.cgi, which allows remote attackers to (1) change the admin password via the admin\_password parameter, (2) disable the security requirement for the Wi-Fi network via unspecified vectors, or (3) modify DNS settings via unspecified vectors.

**References**





▼ URL

Tags

Impacted products

Vendor	Product	Version
<a href="#">dlink</a>	<a href="#">dir-615</a>	3.10na

JSON

Share

To clipboard

Vulnerability from [fkie\\_nvd](#)

Published

2025-08-01 21:15

Modified

2025-09-23 17:38

Severity ?

8.8 (High) - [CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H](#)

Summary

An OS command injection vulnerability exists in multiple D-Link routers—confirmed on DIR-300 rev A (v1.05) and DIR-615 rev D (v4.13)—via the authenticated tools\_vct.cgi CGI endpoint. The web interface fails to properly sanitize user-supplied input in the pingIp parameter, allowing attackers with valid credentials to inject arbitrary shell commands. Exploitation enables full device compromise, including spawning a telnet daemon and establishing a root shell. The vulnerability is present in firmware versions that expose tools\_vct.cgi and use the Mathopd/1.5p6 web server. No vendor patch is available, and affected models are end-of-life.

References

▼ URL

Tags

Impacted products

Vendor	Product	Version
<a href="#">dlink</a>	<a href="#">dir-300_firmware</a>	*
<a href="#">dlink</a>	<a href="#">dir-300</a>	a
<a href="#">dlink</a>	<a href="#">dir-615_firmware</a>	*

33 of 50

13/10/25, 10:53

Vendor	Product	Version
<a href="#">dlink</a>	<a href="#">dir-615</a>	d

JSON

Share

To clipboard

Vulnerability from [fkie\\_nvd](#)

**Published**  
2017-07-19 07:29

**Modified**  
2025-04-20 01:37

**Severity ?**  
9.8 (Critical) - [CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H](#)

**Summary**  
D-Link DIR-615 before v20.12PTb04 has a second admin account with a 0x1 BACKDOOR value, which might allow remote attackers to obtain access via a TELNET connection.

**References**

▼ URL

Tags

**Impacted products**

Vendor	Product	Version
<a href="#">dlink</a>	<a href="#">dir-615</a>	*
<a href="#">dlink</a>	<a href="#">dir-615</a>	*

JSON

Share

To clipboard

Vulnerability from [fkie\\_nvd](#)

**Published**  
2017-07-07 12:29

**Modified**  
2025-04-20 01:37

**Severity ?**



8.8 (High) - [CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H](#)

Summary

On the D-Link DIR-615 before v20.12PTb04, if a victim logged in to the Router's Web Interface visits a malicious site from another Browser tab, the malicious site then can send requests to the victim's Router without knowing the credentials (CSRF). An attacker can host a page that sends a POST request to Form2File.htm that tries to upload Firmware to victim's Router. This causes the router to reboot/crash resulting in Denial of Service. An attacker may succeed in uploading malicious Firmware.

References

▼ URL

Tags

Impacted products

Vendor	Product	Version
<a href="#">dlink</a>	<a href="#">dir-615</a>	*
<a href="#">dlink</a>	<a href="#">dir-615</a>	-

JSON

Share

To clipboard

Vulnerability from [fkie\\_nvd](#)

Published

2019-12-18 13:15

Modified

2024-11-21 04:35

Severity ?

4.8 (Medium) - [CVSS:3.1/AV:N/AC:L/PR:H/UI:R/S:C/C:L/I:L/A:N](#)

Summary

On D-Link DIR-615 devices, the User Account Configuration page is vulnerable to blind XSS via the name field.

References

▼ URL

Tags

Impacted products

Vendor	Product	Version
--------	---------	---------



Vendor	Product	Version
<a href="#">dlink</a>	<a href="#">dir-615_firmware</a>	20.07
<a href="#">dlink</a>	<a href="#">dir-615</a>	-

JSON

Share

To clipboard

Vulnerability from [fkie\\_nvd](#)

**Published**  
2015-05-01 15:59

**Modified**  
2025-04-12 10:46

**Severity ?**  
9.8 (Critical) - [CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H](#)  
9.8 (Critical) - [CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H](#)

**Summary**  
The miniigd SOAP service in Realtek SDK allows remote attackers to execute arbitrary code via a crafted NewInternalClient request, as exploited in the wild through 2023.

**References**

▼ URL

Tags

**Impacted products**

Vendor	Product	Version
<a href="#">dlink</a>	<a href="#">dir-905l_firmware</a>	*
<a href="#">dlink</a>	<a href="#">dir-905l</a>	a1
<a href="#">dlink</a>	<a href="#">dir-905l</a>	b1
<a href="#">dlink</a>	<a href="#">dir-605l_firmware</a>	*
<a href="#">dlink</a>	<a href="#">dir-605l</a>	a1
<a href="#">dlink</a>	<a href="#">dir-600l_firmware</a>	*
<a href="#">dlink</a>	<a href="#">dir-600l</a>	a1
<a href="#">dlink</a>	<a href="#">dir-619l_firmware</a>	*

Vendor	Product	Version
<a href="#">dlink</a>	<a href="#">dir-619l</a>	a1
<a href="#">dlink</a>	<a href="#">dir-619l_firmware</a>	*
<a href="#">dlink</a>	<a href="#">dir-619l</a>	b1
<a href="#">dlink</a>	<a href="#">dir-605l_firmware</a>	*
<a href="#">dlink</a>	<a href="#">dir-605l</a>	b1
<a href="#">dlink</a>	<a href="#">dir-605l_firmware</a>	*
<a href="#">dlink</a>	<a href="#">dir-605l</a>	c1
<a href="#">dlink</a>	<a href="#">dir-600l_firmware</a>	*
<a href="#">dlink</a>	<a href="#">dir-600l</a>	b1
<a href="#">dlink</a>	<a href="#">dir-809_firmware</a>	*
<a href="#">dlink</a>	<a href="#">dir-809</a>	a1
<a href="#">dlink</a>	<a href="#">dir-809</a>	a2
<a href="#">dlink</a>	<a href="#">dir-900l_firmware</a>	*
<a href="#">dlink</a>	<a href="#">dir-900l</a>	a1
<a href="#">realtek</a>	<a href="#">realtek_sdk</a>	-
<a href="#">dlink</a>	<a href="#">dir-501_firmware</a>	*
<a href="#">dlink</a>	<a href="#">dir-501</a>	a1
<a href="#">dlink</a>	<a href="#">dir-515_firmware</a>	*
<a href="#">dlink</a>	<a href="#">dir-515</a>	a1
<a href="#">dlink</a>	<a href="#">dir-615_firmware</a>	10.01b02
<a href="#">dlink</a>	<a href="#">dir-615</a>	j1
<a href="#">dlink</a>	<a href="#">dir-615_firmware</a>	*
<a href="#">dlink</a>	<a href="#">dir-615</a>	fx
<a href="#">aterm</a>	<a href="#">wg1900hp2_firmware</a>	*



Vendor	Product	Version
<a href="#">aterm</a>	<a href="#">wg1900hp2</a>	-
<a href="#">aterm</a>	<a href="#">wg1900hp_firmware</a>	*
<a href="#">aterm</a>	<a href="#">wg1900hp</a>	-
<a href="#">aterm</a>	<a href="#">wg1800hp4_firmware</a>	*
<a href="#">aterm</a>	<a href="#">wg1800hp4</a>	-
<a href="#">aterm</a>	<a href="#">wg1800hp3_firmware</a>	*
<a href="#">aterm</a>	<a href="#">wg1800hp3</a>	-
<a href="#">aterm</a>	<a href="#">wg1200hs2_firmware</a>	*
<a href="#">aterm</a>	<a href="#">wg1200hs2</a>	-
<a href="#">aterm</a>	<a href="#">wg1200hp3_firmware</a>	*
<a href="#">aterm</a>	<a href="#">wg1200hp3</a>	-
<a href="#">aterm</a>	<a href="#">wg1200hp2_firmware</a>	*
<a href="#">aterm</a>	<a href="#">wg1200hp2</a>	-
<a href="#">aterm</a>	<a href="#">w1200ex_firmware</a>	*
<a href="#">aterm</a>	<a href="#">w1200ex</a>	-
<a href="#">aterm</a>	<a href="#">w1200ex-ms_firmware</a>	*
<a href="#">aterm</a>	<a href="#">w1200ex-ms</a>	-
<a href="#">aterm</a>	<a href="#">wg1200hs_firmware</a>	*
<a href="#">aterm</a>	<a href="#">wg1200hs</a>	-
<a href="#">aterm</a>	<a href="#">wg1200hp_firmware</a>	*
<a href="#">aterm</a>	<a href="#">wg1200hp</a>	-
<a href="#">aterm</a>	<a href="#">wf800hp_firmware</a>	*
<a href="#">aterm</a>	<a href="#">wf800hp</a>	-
<a href="#">aterm</a>	<a href="#">wf300hp2_firmware</a>	*



Vendor	Product	Version
<a href="#">aterm</a>	<a href="#">wf300hp2</a>	-
<a href="#">aterm</a>	<a href="#">wr8165n_firmware</a>	*
<a href="#">aterm</a>	<a href="#">wr8165n</a>	-
<a href="#">aterm</a>	<a href="#">w500p_firmware</a>	*
<a href="#">aterm</a>	<a href="#">w500p</a>	-
<a href="#">aterm</a>	<a href="#">w300p_firmware</a>	*
<a href="#">aterm</a>	<a href="#">w300p</a>	-

JSON

Share

To clipboard

Vulnerability from [fkie\\_nvd](#)

**Published**  
2020-04-21 19:15

**Modified**  
2024-11-21 04:32

**Severity ?**  
8.8 (High) - [CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H](#)

**Summary**  
The login page on D-Link DIR-615 T1 20.10 devices allows remote attackers to bypass the CAPTCHA protection mechanism and conduct brute-force attacks.

**References**

▼ URL

Tags

**Impacted products**

Vendor	Product	Version
<a href="#">dlink</a>	<a href="#">dir-615_firmware</a>	20.10
<a href="#">dlink</a>	<a href="#">dir-615</a>	t1

JSON

Share

To clipboard

### [var-201912-1419](#)

Vulnerability from [variot](#)

On D-Link DIR-615 devices, the User Account Configuration page is vulnerable to blind XSS via the name field. D-Link DIR-615 The device contains a cross-site scripting vulnerability. Information may be obtained and information may be altered. D-Link DIR-615 is a wireless router from Taiwan D-Link Corporation. The vulnerability stems from the lack of proper validation of client data by web applications. An attacker could use this vulnerability to execute client code

[Show details on source website](#)

JSON

Share

To clipboard

### [var-202401-0959](#)

Vulnerability from [variot](#)

A vulnerability classified as critical was found in D-Link DAP-1360, DIR-300, DIR-615, DIR-615GF, DIR-615S, DIR-615T, DIR-620, DIR-620S, DIR-806A, DIR-815, DIR-815AC, DIR-815S, DIR-816, DIR-820, DIR-822, DIR-825, DIR-825AC, DIR-825ACF, DIR-825ACG1, DIR-841, DIR-842, DIR-842S, DIR-843, DIR-853, DIR-878, DIR-882, DIR-1210, DIR-1260, DIR-2150, DIR-X1530, DIR-X1860, DSL-224, DSL-245GR, DSL-2640U, DSL-2750U, DSL-G2452GR, DVG-5402G, DVG-5402G, DVG-5402GFRU, DVG-N5402G, DVG-N5402G-IL, DWM-312W, DWM-321, DWR-921, DWR-953 and Good Line Router v2 up to 20240112. This vulnerability affects unknown code of the file /devinfo of the component HTTP GET Request Handler. The manipulation of the argument area with the input notice|net|version leads to information disclosure. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used. VDB-251542 is the identifier assigned to this vulnerability. dir-825acg1 firmware, DIR-841 firmware, dir-1260 firmware etc. D-Link Systems, Inc. There are unspecified vulnerabilities in the product. Information may be obtained





[Show details on source website](#)

JSON

Share

To clipboard

### [var-202108-1937](#)

Vulnerability from [variot](#)

A buffer overflow in D-Link DIR-615 C2 3.03WW. The ping\_ipaddr parameter in ping\_response.cgi POST request allows an attacker to crash the webserver and might even gain remote code execution. D-Link DIR-615 C2 Contains a classic buffer overflow vulnerability. Information is obtained, information is tampered with, and service is disrupted (DoS) It may be put into a state. D-Link DIR-615 is a wireless router made by D-Link in Taiwan.

D-Link DIR-615 has a security vulnerability, which is caused by incorrectly verifying the data boundary when the network system or product performs operations on the memory, resulting in incorrect read and write operations to other associated memory locations. Attackers can use this vulnerability to cause buffer overflow or heap overflow, etc

[Show details on source website](#)

JSON

Share

To clipboard



[var-202208-1907](#)Vulnerability from [variot](#)

The WAN configuration page "wan.htm" on D-Link DIR-615 devices with firmware 20.06 can be accessed directly without authentication which can lead to disclose the information about WAN settings and also leverage attacker to modify the data fields of page. DIR-615 firmware, DIR-615 J1 firmware, dir-615 t1 firmware etc. D-Link Systems, Inc. There are unspecified vulnerabilities in the product. Information is obtained, information is tampered with, and service operation is interrupted. (DoS) It may be in a state

[Show details on source website](#)

JSON

Share

To clipboard

[var-201808-0266](#)Vulnerability from [variot](#)

Cross-site scripting (XSS) vulnerability on D-Link DIR-615 routers 20.07 allows an attacker to inject JavaScript into the "Status -> Active Client Table" page via the hostname field in a DHCP request. D-Link DIR-615 The router contains a cross-site scripting vulnerability. Information may be obtained and information may be altered. D-Link DIR-615 is a small wireless router product from D-Link. A cross-site scripting vulnerability exists in D-Link DIR-615 20.07

[Show details on source website](#)

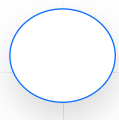
JSON

Share

To clipboard

[var-201910-1280](#)Vulnerability from [variot](#)

An issue discovered on D-Link DIR-615 devices with firmware version 20.05 and 20.07. wan.htm can be accessed directly without authentication, which can lead to disclosure of information about the WAN, and can also be leveraged by an attacker to modify the data fields of the page. D-Link DIR-615 There is an authentication vulnerability in the device firmware. Information may be obtained



and information may be altered. D-Link DIR-615 is a wireless router from D-Link, Taiwan. The vulnerability stems from the lack of authentication measures or insufficient authentication strength in network systems or products

[Show details on source website](#)

[JSON](#)[Share](#)[To clipboard](#)

### [var-201707-1079](#)

Vulnerability from [variot](#)

The D-Link DIR-615 device before v20.12PTb04 doesn't use SSL for any of the authenticated pages. Also, it doesn't allow the user to generate his own SSL Certificate. An attacker can simply monitor network traffic to steal a user's credentials and/or credentials of users being added while sniffing the traffic. D-Link DIR-615 The device contains cryptographic vulnerabilities. Information is obtained, information is altered, and service operation is disrupted (DoS) There is a possibility of being put into a state. D-Link DIR-615 is a small wireless router product of D-Link. There is a security vulnerability in D-Link DIR-615 versions prior to 20.12PTb04

[Show details on source website](#)

[JSON](#)[Share](#)[To clipboard](#)

### [var-201909-0903](#)

Vulnerability from [variot](#)

Unauthenticated remote code execution occurs in D-Link products such as DIR-655C, DIR-866L, DIR-652, and DHP-1565. The issue occurs when the attacker sends an arbitrary input to a "PingTest" device common gateway interface that could lead to common injection. An attacker who successfully triggers the command injection could achieve full system compromise. Later, it was independently found that these are also affected: DIR-855L, DAP-1533, DIR-862L, DIR-615, DIR-835, and DIR-825. plural D-Link The product includes OS A command injection vulnerability exists. Information is obtained, information is altered, and service operation is disrupted (DoS) There is a possibility of being put into a



state. D-Link DIR-655C, etc. are all wireless routers from Taiwan D-Link. Attackers can use this vulnerability to inject commands to invade the system. The following products and versions are affected: D-Link DIR-655C; DIR-866L; DIR-652; DHP-1565, etc.

Exploiting this issue could allow an malicious user to execute arbitrary commands in the context of the affected device. Failed exploit attempts will likely result in denial-of-service conditions

[Show details on source website](#)

[JSON](#)[Share](#)[To clipboard](#)

### [var-201707-1077](#)

Vulnerability from [variot](#)

On the D-Link DIR-615 before v20.12PTb04, if a victim logged in to the Router's Web Interface visits a malicious site from another Browser tab, the malicious site then can send requests to the victim's Router without knowing the credentials (CSRF). An attacker can host a page that sends a POST request to Form2File.htm that tries to upload Firmware to victim's Router. This causes the router to reboot/crash resulting in Denial of Service. An attacker may succeed in uploading malicious Firmware. D-Link DIR-615 Contains a cross-site request forgery vulnerability. Information is obtained, information is altered, and service operation is disrupted (DoS) There is a possibility of being put into a state. D-Link DIR-615 is a small wireless router product of D-Link. A security vulnerability exists in versions prior to D-Link DIR-615 20.12PTb04

[Show details on source website](#)

[JSON](#)[Share](#)[To clipboard](#)

### [var-201004-0071](#)

Vulnerability from [variot](#)

The D-Link DIR-615 with firmware 3.10NA does not require administrative authentication for apply.cgi, which allows remote attackers to (1) change the admin password via the admin\_password parameter, (2) disable the security requirement for the Wi-Fi



network via unspecified vectors, or (3) modify DNS settings via unspecified vectors. D-Link DIR-615 Is apply.cgi The following vulnerabilities exist because management authentication for is not required. The D-Link DIR-615 is a small wireless router. The DIR-615 router does not restrict access to the apply.cgi script. D-Link DIR-615 is is prone to a security-bypass vulnerability. Remote attackers can exploit this issue to bypass security restrictions and access certain administrative functions.

-----

Do you have VARM strategy implemented?

(Vulnerability Assessment Remediation Management)

If not, then implement it through the most reliable vulnerability intelligence source on the market.

Implement it through Secunia.

For more information visit: [http://secunia.com/advisories/business\\_solutions/](http://secunia.com/advisories/business_solutions/)

Alternatively request a call from a Secunia representative today to discuss how we can help you with our capabilities contact us at: [sales@secunia.com](mailto:sales@secunia.com)

---

TITLE: D-Link DIR-615 "apply.cgi" Security Bypass Vulnerability

SECUNIA ADVISORY ID: SA37777

VERIFY ADVISORY: <http://secunia.com/advisories/37777/>

DESCRIPTION: gerry has reported a vulnerability in D-Link DIR-615, which can be exploited by malicious people to bypass certain security restrictions. This can be exploited to e.g. change the administrator password via a specially crafted HTTP request.

The vulnerability is reported in firmware version 3.10NA. Other versions may also be affected.

PROVIDED AND/OR DISCOVERED BY: gerry

ORIGINAL ADVISORY: <http://www.hiredhacker.com/2009/12/15/d-link-dir-615-remote-exploit/>

---

About: This Advisory was delivered by Secunia as a free service to



help everybody keeping their systems up to date against the latest vulnerabilities.

Subscribe: [http://secunia.com/advisories/secunia\\_security\\_advisories/](http://secunia.com/advisories/secunia_security_advisories/)

Definitions: (Criticality, Where etc.) [http://secunia.com/advisories/about\\_secunia\\_advisories/](http://secunia.com/advisories/about_secunia_advisories/)

Please Note: Secunia recommends that you verify all advisories you receive by clicking the link. Secunia NEVER sends attached files with advisories. Secunia does not advise people to install third party patches, only use those supplied by the vendor.

---

Unsubscribe: Secunia Security Advisories [http://secunia.com/sec\\_adv\\_unsubscribe/?email=packet%40packetstormsecurity.org](http://secunia.com/sec_adv_unsubscribe/?email=packet%40packetstormsecurity.org)

---

[Show details on source website](#)

JSON

Share

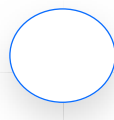
To clipboard

### [var-201707-1078](#)

Vulnerability from [variot](#)

On the D-Link DIR-615 before v20.12PTb04, once authenticated, this device identifies the user based on the IP address of his machine. By spoofing the IP address belonging to the victim's host, an attacker might be able to take over the administrative session without being prompted for authentication credentials. An attacker can get the victim's and router's IP addresses by simply sniffing the network traffic. Moreover, if the victim has web access enabled on his router and is accessing the web interface from a different network that is behind the NAT/Proxy, an attacker can sniff the network traffic to know the public IP address of the victim's router and take over his session as he won't be prompted for credentials. D-Link DIR-615 Contains an authentication vulnerability. Information is obtained, information is altered, and service operation is disrupted (DoS) There is a possibility of being put into a state. D-Link DIR-615 is a small wireless router product of D-Link.

D-Link DIR-615 has an authorization issue vulnerability. A security vulnerability exists in versions prior to D-Link DIR-615 20.12PTb04



[Show details on source website](#)

JSON

Share

To clipboard

### [var-202004-0708](#)

Vulnerability from [variot](#)

The login page on D-Link DIR-615 T1 20.10 devices allows remote attackers to bypass the CAPTCHA protection mechanism and conduct brute-force attacks. D-Link DIR-615 T1 The device is vulnerable to improper restrictions on excessive authentication attempts. Information is obtained, information is tampered with, and service operation is interrupted. (DoS) It may be put into a state. D-Link DIR-615 is a wireless router from D-Link, Taiwan.

D-Link DIR-615 T1 20.10 version of the login page has a security vulnerability

[Show details on source website](#)

JSON

Share

To clipboard

### [var-201505-0274](#)

Vulnerability from [variot](#)

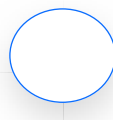
The miniigd SOAP service in Realtek SDK allows remote attackers to execute arbitrary code via a crafted NewInternalClient request, as exploited in the wild through 2023. The following multiple vulnerabilities exist in multiple products provided by ELECOM CORPORATION.

- Inadequate access restrictions (CWE-284) - CVE-2021-20643
- Script injection on the management screen (CWE-74) - CVE-2021-20644
- Retractable cross-site scripting (CWE-79) - CVE-2021-20645
- Cross-site request forgery (CWE-352) - CVE-2021-20646, CVE-2021-20647, CVE-2021-20650
- OS Command injection (CWE-78) - CVE-2021-20648
- Insufficient verification of server certificate (CWE-295) - CVE-2021-20649
- UPnP Via OS Command injection (CWE-78) - CVE-2014-8361

CVE-2021-20643 This vulnerability information is based on the Information Security Early Warning Partnership. IPA Report to JPCERT/CC Coordinated with the developer. Reporter : Institute of



Information Security Yuasa Laboratory Nagakawa ( Ishibashi )  
Australia Mr CVE-2021-20644 This vulnerability information is based on the Information Security Early Warning Partnership. IPA Report to JPCERT/CC Coordinated with the developer. Reporter : Sato Rei Mr CVE-2021-20645, CVE-2021-20646 These vulnerability information is based on the Information Security Early Warning Partnership. IPA Report to JPCERT/CC Coordinated with the developer. Reporter : Mitsui Bussan Secure Direction Co., Ltd. Tetsuyuki Ogawa Mr CVE-2021-20647, CVE-2021-20648, CVE-2021-20649 These vulnerability information is based on the Information Security Early Warning Partnership. IPA Report to JPCERT/CC Coordinated with the developer. Reporter : Cyber Defense Institute, Inc. Satoru Nagaoka Mr CVE-2021-20650 This vulnerability information is based on the Information Security Early Warning Partnership. IPA Report to JPCERT/CC Coordinated with the developer. Reporter : Hiroshi Watanabe Mr CVE-2014-8361 The following person indicates that the product is vulnerable to IPA Report to JPCERT/CC Coordinated with the developer. Reporter : Cyber Defense Institute, Inc. Satoru Nagaoka Mr., National Institute of Information and Communications Technology Makita Daisuke Mr., National Institute of Information and Communications Technology Woods Yoshiki MrThe expected impact depends on each vulnerability, but it may be affected as follows. -The management password of the product is changed by processing the request crafted by a remote third party. - CVE-2021-20643 • Crafted SSID Is displayed on the management screen, and any script is executed on the user's web browser. - CVE-2021-20644 -Any script is executed on the web browser of the user who is logged in to the product. - CVE-2021-20645 -When a user logged in to the management screen of the product accesses a specially crafted page, an arbitrary request is executed, and as a result, the settings of the product are changed unintentionally. telnet Daemon is started - CVE-2021-20646, CVE-2021-20647, CVE-2021-20650 • Any third party who can access the product OS Command is executed - CVE-2021-20648 • Man-in-the-middle attack (man-in-the-middle attack) The communication response has been tampered with, resulting in arbitrary in the product. OS Command is executed - CVE-2021-20649 • With the product UPnP Is valid, any by a third party who has access to the product OS Command is executed - CVE-2014-8361. Provided by Buffalo Co., Ltd. WSR-300HP is wireless LAN It's a router. Authentication is not required to exploit this vulnerability.The specific flaw exists within





the miniigd SOAP service. The issue lies in the handling of the NewInternalClient requests due to a failure to sanitize user data before executing a system call. An attacker could leverage this vulnerability to execute code with root privileges. Failed exploit attempts will result in a denial-of-service condition. Realtek SDK is a set of SDK development kit developed by Realtek

[Show details on source website](#)

JSON

Share

To clipboard

### [var-201707-0541](#)

Vulnerability from [variot](#)

D-Link DIR-615 before v20.12PTb04 has a second admin account with a 0x1 BACKDOOR value, which might allow remote attackers to obtain access via a TELNET connection. D-Link DIR-615 Contains a vulnerability in the use of hard-coded credentials. Information is obtained, information is altered, and service operation is disrupted (DoS) There is a possibility of being put into a state. D-LinkDIR-615 is a small wireless router product from D-Link. A security vulnerability exists in versions prior to D-LinkDIR-61520.12PTb04

[Show details on source website](#)

JSON

Share

To clipboard

### [var-201808-0267](#)

Vulnerability from [variot](#)

Cross-site scripting (XSS) vulnerability on D-Link DIR-615 routers 20.07 allows attackers to inject JavaScript into the router's admin UPnP page via the description field in an AddPortMapping UPnP SOAP request. D-Link DIR-615 The router contains a cross-site scripting vulnerability. Information may be obtained and information may be altered. D-LinkDIR-615 is a small wireless router product from D-Link. A cross-site scripting vulnerability exists in D-LinkDIR-61520.07

[Show details on source website](#)



JSON

Share

To clipboard

[var-202109-1681](#)Vulnerability from [variot](#)

An information disclosure issue exist in D-LINK-DIR-615 B2 2.01mt. An attacker can obtain a user name and password by forging a post request to the / getcfg.php page. D-LINK-DIR-615 Exists in a fraudulent authentication vulnerability. Information may be obtained. D-Link DIR-615 is a SOHO wireless router with a maximum transmission rate of 300Mbps

[Show details on source website](#)

JSON

Share

To clipboard

[var-201808-0206](#)Vulnerability from [variot](#)

D-Link DIR-615 devices have a buffer overflow via a long Authorization HTTP header. D-Link DIR-615 Devices contain a buffer error vulnerability. Information is obtained, information is altered, and service operation is disrupted (DoS) There is a possibility of being put into a state. D-LinkDIR-615 is a small wireless router product from D-Link. A buffer overflow vulnerability exists in D-LinkDIR-615. An attacker could exploit the vulnerability with a longer Authorization HTTP header to log off the router and cause a network outage

[Show details on source website](#)

JSON

Share

To clipboard

