

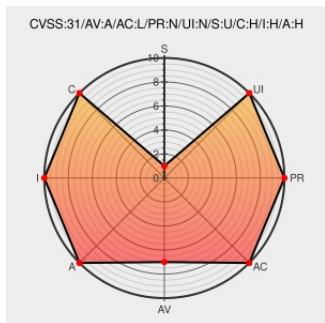


CVE-2021-29379

Published on: 04/12/2021 12:00:00 AM UTC

Last Modified on: 04/19/2021 04:39:00 PM UTC

CVE-2021-29379

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

Certain versions of [Dir-802](#) from [Dlink](#) contain the following vulnerability:

**** UNSUPPORTED WHEN ASSIGNED **** An issue was discovered on D-Link DIR-802 A1 devices through 1.00b05. Universal Plug and Play (UPnP) is enabled by default on port 1900. An attacker can perform command injection by injecting a payload into the Search Target (ST) field of the SSDP M-SEARCH discover packet. NOTE: This vulnerability only affects products that are no longer supported by the maintainer.

CVE-2021-29379 has been assigned by [M](#) cve@mitre.org to track the vulnerability - currently rated as **HIGH** severity.

CVSS3 Score: **8.8 - HIGH**

Attack Vector	Attack Complexity	Privileges Required	User Interaction
ADJACENT_NETWORK	LOW	NONE	NONE
Scope	Confidentiality Impact	Integrity Impact	Availability Impact
UNCHANGED	HIGH	HIGH	HIGH

CVSS2 Score: **5.8 - MEDIUM**

Access Vector	Access Complexity	Authentication
ADJACENT_NETWORK	LOW	NONE
Confidentiality Impact	Integrity Impact	Availability Impact
PARTIAL	PARTIAL	PARTIAL

CVE References

Description	Tags	Link
Security Bulletin D-Link	www.dlink.com text/html	MISC www.dlink.com/en/security-bulletin/

DIR-802 OS Command Injection
| 混元霹雳手

cool-y.github.io
text/html

MISC cool-y.github.io/2021/03/02/DIR-802-OS-Command-Injection

D-Link Technical Support

supportannouncement.us.dlink.com
text/html

MISC
supportannouncement.us.dlink.com/announcement/publication.aspx?name=SAP10206

By selecting these links, you may be leaving CVEreport webspace. We have provided these links to other websites because they may have information that would be of interest to you. No inferences should be drawn on account of other sites being referenced, or not, from this page. There may be other websites that are more appropriate for your purpose. CVEreport does not necessarily endorse the views expressed, or concur with the facts presented on these sites. Further, CVEreport does not endorse any commercial products that may be mentioned on these sites. Please address comments about any linked pages to comment@cve.report.

There are currently no QIDs associated with this CVE

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Hardware 	Dlink	Dir-802	a1	All	All	All
Operating System	Dlink	Dir-802 Firmware	All	All	All	All
cpe:2.3:h:dlink:dir-802:a1:*.***.***.***:						
cpe:2.3:o:dlink:dir-802_firmware:*.***.***.***:						

No vendor comments have been submitted for this CVE

Social Mentions

Source	Title	Posted (UTC)
 @CVEreport	CVE-2021-29379 : An issue was discovered on D-Link DIR-802 A1 devices through 1.00b05. Universal Plug and Play U... twitter.com/i/web/status/1...	2021-04-12 05:06:37
 @SystemTek_UK	D-Link DIR-802 Command Injection Vulnerability [CVE-2021-29379] systemtek.co.uk/2021/04/d-link...	2021-04-12 13:52:03
 @6townstechteam	D-Link DIR-802 Command Injection Vulnerability [CVE-2021-29379] systemtek.co.uk/2021/04/d-link...	2021-04-12 13:52:05
 @Har_sia	CVE-2021-29379 har-sia.info/CVE-2021-29379... #HarsiaInfo	2021-04-12 18:25:03

[← Previous ID](#)

[Next ID →](#)

© CVE.report 2023  |

Use of this information constitutes acceptance for use in an AS IS condition. There are NO warranties, implied or otherwise, with regard to this information or its use. Any use of this information is at the user's risk. It is the responsibility of user to evaluate the accuracy, completeness or usefulness of any information, opinion, advice or other content. EACH USER WILL BE SOLELY RESPONSIBLE FOR ANY consequences of his or her direct or indirect use of this web site. ALL WARRANTIES OF ANY KIND ARE EXPRESSLY DISCLAIMED. This site will NOT BE LIABLE FOR ANY DIRECT, INDIRECT or any other kind of loss.

CVE, CWE, and OVAL are registered trademarks of [The MITRE Corporation](#) and the authoritative source of CVE content is [MITRE's CVE web site](#). This site includes MITRE data granted under the following [license](#).

