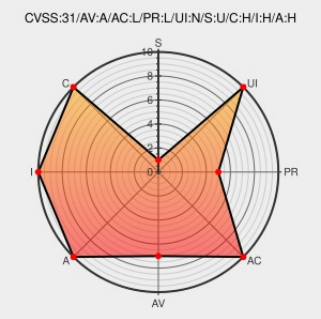
CVE-2020-24581

Published on: 12/22/2020 12:00:00 AM UTC

Last Modified on: 04/26/2023 07:27:00 PM UTC

CVE-2020-24581

Source: Mitre | Source: NIST | CVE.ORG | Print: PDF



Certain versions of Dsl2888a from D-link contain the following vulnerability:

An issue was discovered on D-Link DSL-2888A devices with firmware prior to AU_2.31_V1.1.47ae55. It contains an execute_cmd.cgi feature (that is not reachable via the web user interface) that lets an authenticated user execute Operating System commands.

CVE-2020-24581 has been assigned by cve@mitre.org to track the vulnerability - currently rated as HIGH severity.

CVSS3 Score: 8 - HIGH

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

CVSS2 Score: 7.7 - HIGH

Access Vector	Access Complexity	Authentication
ADJACENT_NETWORK	LOW	SINGLE
Confidentiality Impact	**Integrity Impact**	**Availability Impact**
COMPLETE	COMPLETE	COMPLETE

CVE References

Description	Tags	Link
Security Advisories | Trustwave	Third Party Advisory, www.trustwave.com, text/html	CONFIRM www.trustwave.com/en-us/resources/security-resources/security-advisories/
D-Link: Multiple Security Vulnerabilities	Exploit	MISC www.trustwave.com/en-us/resources/blogs/spiderlabs-blog/d-

Leading to RCE | Trustwave	Third Party Advisory www.trustwave.com text/html	link-multiple-security-vulnerabilities-leading-to-rce/

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	D-link	Dsl2888a	-	All	All	All
Hardware	D-link	Dsl2888a	-	All	All	All
Operating System	D-link	Dsl2888a Firmware	All	All	All	All
Operating System	D-link	Dsl2888a Firmware	All	All	All	All
Hardware	Dlink	Dsl2888a	-	All	All	All
Operating System	Dlink	Dsl2888a Firmware	All	All	All	All

cpe:2.3:h:d-link:dsl2888a:-:*:*:*:*:*:*:*:

cpe:2.3:h:d-link:dsl2888a:-:*:*:*:*:*:*:*:

cpe:2.3:o:d-link:dsl2888a_firmware:*:*:*:*:*:*:*:*:

cpe:2.3:o:d-link:dsl2888a_firmware:*:*:*:*:*:*:*:*:

cpe:2.3:h:dlink:dsl2888a:-:*:*:*:*:*:*:*:

cpe:2.3:o:dlink:dsl2888a_firmware:*:*:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

Social Mentions

Source	Title	Posted (UTC)
@reverseame	CVE-2020-24581 D-Link DSL-2888A Remote Command Execution reconshell.com/cve-2020-24581…	2021-04-12 14:37:44
@ipssignatures	It's new to me that Hillstone has a protection/signature/rule for the vulnerability CVE-2020-24581.… twitter.com/i/web/status/1…	2021-07-08 11:02:00
@ipssignatures	It is the first time for me to know a protection/signature/rule for the vulnerability CVE-2020-24581. #Sl7w56e7vxgs24	2021-07-08 11:02:01
@ptracesecurity	CVE-2020-24581 D-Link DSL-2888A Remote Command Execution reconshell.com/cve-2020-24581 #Pentesting #CVE #Dlink #RCE twitter.com/i/web/status/1	2021-09-05 06:03:51

@ptracesecurity	24581… #Pentesting #CVE #DLink #RCE… twitter.com/i/web/status/1…	06:06:54
@cKure7	■■■□□ CVE-2020-24581 D-Link DSL-2888A Remote Command Execution reconshell.com/cve-2020-24581…	2021-09-05 06:25:50
@ipssignatures	The vuln CVE-2020-24581 has a tweet created 0 days ago and retweeted 14 times. twitter.com/ptracesecurity… #pow1rtrtwwcve	2021-09-05 09:06:00

← 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 registred 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.

CVE.report and Source URL Uptime Status status.cve.report