



CVE-2020-9544

Published on: 03/05/2020 12:00:00 AM UTC

Last Modified on: 07/21/2021 11:39:00 AM UTC

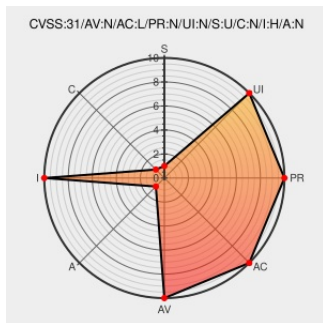
CVE-2020-9544

Source: Mitre

Source: NIST

CVE.ORG

Print: PDF



Certain versions of [Dsl-2640b](#) from [D-link](#) contain the following vulnerability:

An issue was discovered on D-Link DSL-2640B E1 EU_1.01 devices. The administrative interface doesn't perform authentication checks for a firmware-update POST request. Any attacker that can access the administrative interface can install firmware of their choice.

CVE-2020-9544 has been assigned by [M](#) cve@mitre.org to track the vulnerability - currently rated as **HIGH** severity.

CVSS3 Score: **7.5 - HIGH**

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

CVSS2 Score: **5 - MEDIUM**

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



CVE References

Description	Tags	Link
CVE-2020-9544: DLink DSL-2640B un-authenticated firmware upgrade · Gianluca Pacchiella	Exploit Third Party Advisory ktln2.org text/html	MISC ktln2.org/2020/03/05/cve-2020-9544/

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	Dsl-2640b	-	All	All	All
Hardware 	D-link	Dsl-2640b	-	All	All	All
Operating System	D-link	Dsl-2640b Firmware	e1_eu_1.01	All	All	All
Operating System	D-link	Dsl-2640b Firmware	e1_eu_1.01	All	All	All
<code>cpe:2.3:h:d-link:dsl-2640b:-:*:*:*:*:*:</code>						
<code>cpe:2.3:h:d-link:dsl-2640b:-:*:*:*:*:*:</code>						
<code>cpe:2.3:o:d-link:dsl-2640b_firmware:e1_eu_1.01:*:*:*:*:*:</code>						
<code>cpe:2.3:o:d-link:dsl-2640b_firmware:e1_eu_1.01:*:*:*:*:*:</code>						

No vendor comments have been submitted for this CVE

[← 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](#).

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