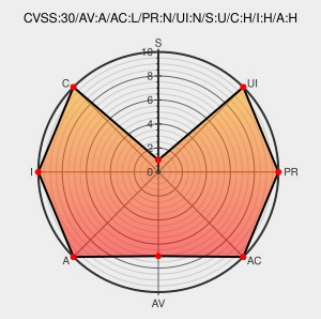
CVE-2019-17146

Published on: 01/07/2020 12:00:00 AM UTC

Last Modified on: 10/29/2021 06:48:00 PM UTC

CVE-2019-17146

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



Certain versions of Dcs-935l from Dlink contain the following vulnerability:

This vulnerability allows remote attackers to execute arbitrary code on affected installations of D-Link DCS-960L v1.07.102. Authentication is not required to exploit this vulnerability. The specific flaw exists within the HNAP service, which listens on TCP port 80 by default. When parsing the SOAPAction request header, the process does not properly validate the length of user-supplied data prior to copying it to a stack-based buffer. An attacker can leverage this vulnerability to execute code in the context of the admin user. Was ZDI-CAN-8458.

CVE-2019-17146 has been assigned by zdi-disclosures@trendmicro.com to track the vulnerability - currently rated as CRITICAL severity.

Affected Vendor/Software: **D-Link** - **DCS-960L** version **v1.07.102**

CVSS3 Score: 9.8 - CRITICAL

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

CVSS2 Score: 10 - HIGH

Access Vector	Access Complexity	Authentication
NETWORK	LOW	NONE
Confidentiality Impact	**Integrity Impact**	**Availability Impact**
COMPLETE	COMPLETE	COMPLETE

CVE References

Description	Tags	Link
ZDI-19-1031 | Zero Day Initiative	Third Party Advisory VDB Entry www.zerodayinitiative.com text/html	N/A N/A
D-Link Technical Support	Vendor Advisory supportannouncement.us.dlink.com text/html	MISC supportannouncement.us.dlink.com/announcement/publication.aspx?name=SAP10142

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	Dcs-935l	-	All	All	All
Hardware	Dlink	Dcs-935l	ax	All	All	All
Hardware	Dlink	Dcs-935l	-	All	All	All
Operating System	Dlink	Dcs-935l Firmware	All	All	All	All
Hardware	Dlink	Dcs-960l	-	All	All	All
Hardware	Dlink	Dcs-960l	a	All	All	All
Hardware	Dlink	Dcs-960l	-	All	All	All
Operating System	Dlink	Dcs-960l Firmware	All	All	All	All

cpe:2.3:h:dlink:dcs-935l:-:*:*:*:*:*:*:*:

cpe:2.3:h:dlink:dcs-935l:ax:*:*:*:*:*:*:*:

cpe:2.3:h:dlink:dcs-935l:-:*:*:*:*:*:*:*:

cpe:2.3:o:dlink:dcs-935l_firmware:*:*:*:*:*:*:*:*:

cpe:2.3:h:dlink:dcs-960l:-:*:*:*:*:*:*:*:

cpe:2.3:h:dlink:dcs-960l:a:*:*:*:*:*:*:*:

cpe:2.3:h:dlink:dcs-960l:-:*:*:*:*:*:*:*:

cpe:2.3:o:dlink:dcs-960l_firmware:*:*:*:*:*:*:*:*:

Discovery Credit

Anonymous

Social Mentions

Source	Title	Posted (UTC)

← Previous ID

Next ID→

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