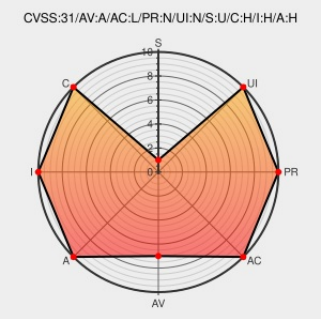
CVE-2019-13263

Published on: 08/27/2019 12:00:00 AM UTC

Last Modified on: 04/27/2023 02:29:00 PM UTC

CVE-2019-13263

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



Certain versions of Dir-825/ac G1 from D-link contain the following vulnerability:

D-link DIR-825AC G1 devices have Insufficient Compartmentalization between a host network and a guest network that are established by the same device. A DHCP Request is sent to the router with a certain Transaction ID field. Following the DHCP protocol, the router responds with an ACK or NAK message. Studying the NAK case revealed that the router erroneously sends the NAK to both Host and Guest networks with the same Transaction ID as found in the DHCP Request. This allows encoding of data to be sent cross-router into the 32-bit Transaction ID field.

CVE-2019-13263 has been assigned by 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

	Third Party Advisory www.usenix.org application/pdf	MISC www.usenix.org/system/files/woot19-paper_ovadia.pdf
Redirecting…	Exploit Third Party Advisory orenlab.sise.bgu.ac.il text/html	MISC orenlab.sise.bgu.ac.il/publications/CrossRouter

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	Dir-825/ac G1	-	All	All	All
Operating System	D-link	Dir-825/ac G1 Firmware	-	All	All	All
Hardware	D-link	Dir-825/ac G1	-	All	All	All
Hardware	D-link	Dir-825/ac G1	-	All	All	All
Operating System	D-link	Dir-825/ac G1 Firmware	-	All	All	All
Operating System	D-link	Dir-825/ac G1 Firmware	-	All	All	All
Hardware	Dlink	Dir-825/ac G1	-	All	All	All
Operating System	Dlink	Dir-825/ac G1 Firmware	-	All	All	All

cpe:2.3:h:d-link:dir-825/ac_g1:-:*:*:*:*:*:*:*:

cpe:2.3:o:d-link:dir-825/ac_g1_firmware:-:*:*:*:*:*:*:*:

cpe:2.3:h:d-link:dir-825\/ac_g1:-:*:*:*:*:*:*:*:

cpe:2.3:h:d-link:dir-825\/ac_g1:-:*:*:*:*:*:*:*:

cpe:2.3:o:d-link:dir-825\/ac_g1_firmware:-:*:*:*:*:*:*:*:

cpe:2.3:o:d-link:dir-825\/ac_g1_firmware:-:*:*:*:*:*:*:*:

cpe:2.3:h:dlink:dir-825\/ac_g1:-:*:*:*:*:*:*:*:

cpe:2.3:o:dlink:dir-825\/ac_g1_firmware:-:*:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→