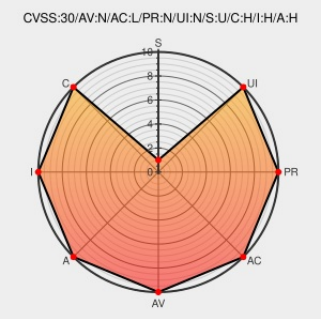
CVE-2017-11563

Published on: 08/24/2018 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:26:24 PM UTC

CVE-2017-11563

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



Certain versions of Eyeon Baby Monitor from Dlink contain the following vulnerability:

D-Link EyeOn Baby Monitor (DCS-825L) 1.08.1 has a remote code execution vulnerability. A UDP "Discover" service, which provides multiple functions such as changing the passwords and getting basic information, was installed on the device. A remote attacker can send a crafted UDP request to finderd to perform stack overflow and execute arbitrary code with root privilege on the device.

CVE-2017-11563 has been assigned by cve@mitre.org to track the vulnerability - currently rated as CRITICAL severity.

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
Full Disclosure:	Mailing List, Third Party Advisory	FULLDISC 20180821 CVE-2017-11563: Remote Code Execution via stack overflow in D-Link EyeOn Baby Monitor (DCS-825L)

CVE-2017-11563: Remote Code Execution via stack overflow in D-Link EyeOn Baby Monitor (DCS-825L)

seclists.org
text/html

Technical Description
Third Party Advisory
documents.trendmicro.com
application/pdf

MISC
documents.trendmicro.com/assets/tech_brief_Device_Vulnerabilities_in_the_Connected_Home2.p

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	Eyeon Baby Monitor	-	All	All	All
Hardware	Dlink	Eyeon Baby Monitor	-	All	All	All
Operating System	Dlink	Eyeon Baby Monitor Firmware	1.08.1	All	All	All
Operating System	Dlink	Eyeon Baby Monitor Firmware	1.08.1	All	All	All

cpe:2.3:h:dlink:eyeon_baby_monitor:-:*:*:*:*:*:*:*:

cpe:2.3:h:dlink:eyeon_baby_monitor:-:*:*:*:*:*:*:*:

cpe:2.3:o:dlink:eyeon_baby_monitor_firmware:1.08.1:*:*:*:*:*:*:*:

cpe:2.3:o:dlink:eyeon_baby_monitor_firmware:1.08.1:*:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→

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