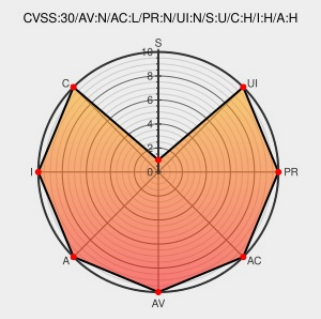
CVE-2017-3192

Published on: 12/15/2017 12:00:00 AM UTC

Last Modified on: 04/26/2023 06:55:00 PM UTC

CVE-2017-3192

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



Certain versions of Dir-130 from D-link contain the following vulnerability:

D-Link DIR-130 firmware version 1.23 and DIR-330 firmware version 1.12 do not sufficiently protect administrator credentials. The tools_admin.asp page discloses the administrator password in base64 encoding in the returned web page. A remote attacker with access to this page (potentially through a authentication bypass such as CVE-2017-3191) may obtain administrator credentials for the device.

CVE-2017-3192 has been assigned by cert@cert.org to track the vulnerability - currently rated as CRITICAL severity.

Affected Vendor/Software: **D-Link** - **DIR-130** version **1.23**

Affected Vendor/Software: **D-Link** - **DIR-330** version **1.12**

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: 5 - MEDIUM

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

CVE References

Description	Tags	Link
VU#553503 - D-Link DIR-130 and DIR-330 are vulnerable to authentication bypass and do not protect credentials	Issue Tracking Third Party Advisory US Government Resource www.kb.cert.org text/html	CERT-VN VU#553503
IBM X-Force Exchange	Issue Tracking Third Party Advisory VDB Entry exchange.xforce.ibmcloud.com text/html	MISC exchange.xforce.ibmcloud.com/vulnerabilities/123292
D-Link DIR-130 and DIR-330 routers vulnerable	Third Party Advisory www.scmagazine.com text/html	MISC www.scmagazine.com/d-link-dir-130-and-dir-330-routers-vulnerable/article/644553/
D-Link DIR-130 and DIR-330 are vulnerable to authentication bypass and do not protect credentials | Wilders Security Forums	Issue Tracking Third Party Advisory www.wilderssecurity.com text/html	MISC www.wilderssecurity.com/threads/d-link-dir-130-and-dir-330-are-vulnerable-to-authentication-bypass-and-do-not-protect-credentials.392703/

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-130	-	All	All	All
Hardware	D-link	Dir-130	-	All	All	All
Operating System	D-link	Dir-130 Firmware	1.23	All	All	All
Operating System	D-link	Dir-130 Firmware	1.23	All	All	All
Hardware	D-link	Dir-330	-	All	All	All
Hardware	D-link	Dir-330	-	All	All	All
Operating System	D-link	Dir-330 Firmware	1.12	All	All	All
Operating System	D-link	Dir-330 Firmware	1.12	All	All	All
Hardware	Dlink	Dir-130	-	All	All	All
Hardware	Dlink	Dir-330	-	All	All	All

cpe:2.3:h:d-link:dir-130:-:*:*:*:*:*:*:*:

cpe:2.3:h:d-link:dir-130:-:*:*:*:*:*:*:*:

cpe:2.3:o:d-link:dir-130_firmware:1.23:*:*:*:*:*:*:*

cpe:2.3:o:d-link:dir-130_firmware:1.23:*:*:*:*:*:*:*

cpe:2.3:h:d-link:dir-330:-:*:*:*:*:*:*:*

cpe:2.3:h:d-link:dir-330:-:*:*:*:*:*:*:*

cpe:2.3:o:d-link:dir-330_firmware:1.12:*:*:*:*:*:*:*

cpe:2.3:o:d-link:dir-330_firmware:1.12:*:*:*:*:*:*:*

cpe:2.3:h:dlink:dir-130:-:*:*:*:*:*:*:*

cpe:2.3:h:dlink:dir-330:-:*:*:*:*:*:*:*

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→