

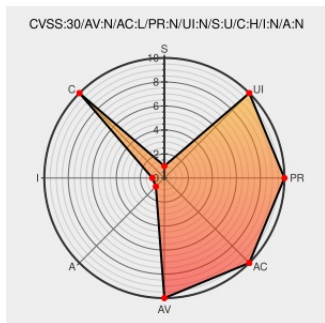


CVE-2015-8289

Published on: 06/19/2016 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:26:13 PM UTC

CVE-2015-8289

[Source: Mitre](#)[Source: NIST](#)[CVE.ORG](#)[Print: PDF](#) 

Certain versions of **D3600** from **Netgear** contain the following vulnerability:

The password-recovery feature on NETGEAR D3600 devices with firmware 1.0.0.49 and D6000 devices with firmware 1.0.0.49 and earlier allows remote attackers to discover the cleartext administrator password by reading the cgi-bin/passrec.asp HTML source code.

CVE-2015-8289 has been assigned by cert@cert.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	HIGH	NONE	NONE

CVSS2 Score: **4.3 - MEDIUM**

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

CVE References

Description	Tags	Link
Vulnerability Note VU#778696 - Netgear D6000 and D3600 contain hard-coded cryptographic keys and are vulnerable to authentication bypass	Third Party Advisory US Government Resource www.kb.cert.org text/html	CERT-VN VU#778696

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  	Netgear	D3600	-	All	All	All
Hardware  	Netgear	D3600	-	All	All	All
Operating System	Netgear	D3600 Firmware	1.0.0.49	All	All	All
Operating System	Netgear	D3600 Firmware	1.0.0.49	All	All	All
Hardware  	Netgear	D6000	-	All	All	All
Hardware  	Netgear	D6000	-	All	All	All
Operating System	Netgear	D6000 Firmware	All	All	All	All
cpe:2.3:h:netgear:d3600:-:~::~~::~~::~~::~~::~~::~~:::						
cpe:2.3:h:netgear:d3600:-:~::~~::~~::~~::~~::~~::~~:::						
cpe:2.3:o:netgear:d3600_firmware:1.0.0.49:~::~~::~~::~~::~~::~~::~~:::						
cpe:2.3:o:netgear:d3600_firmware:1.0.0.49:~::~~::~~::~~::~~::~~::~~:::						
cpe:2.3:h:netgear:d6000:-:~::~~::~~::~~::~~::~~::~~:::						
cpe:2.3:h:netgear:d6000:-:~::~~::~~::~~::~~::~~::~~:::						
cpe:2.3:o:netgear:d6000_firmware:~::~~::~~::~~::~~::~~::~~:::						

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 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](#)