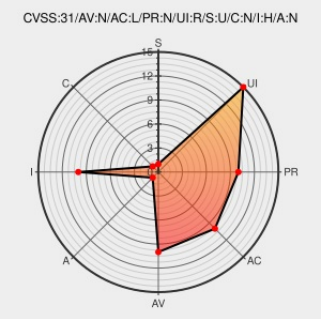
CVE-2016-11015

Published on: 10/15/2019 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:26:59 PM UTC

CVE-2016-11015

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



Certain versions of Jnr1010 from Netgear contain the following vulnerability:

NETGEAR JNR1010 devices before 1.0.0.32 allow cgi-bin/webproc CSRF via the :InternetGatewayDevice.X_TWSZ-COM_URL_Filter.BlackList.1.URL parameter.

CVE-2016-11015 has been assigned by cve@mitre.org to track the vulnerability - currently rated as MEDIUM severity.

CVSS3 Score: 6.5 - MEDIUM

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

CVSS2 Score: 4.3 - MEDIUM

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

CVE References

Description	Tags	Link
[FD] Cross Site Request Forgery in Netgear Router JNR1010 Version 1.0.0.24 – InsideNothing	Third Party Advisory, pmcg2k15.wordpress.com, text/html	MISC pmcg2k15.wordpress.com/2016/01/11/fd-cross-site-request-forgery-in-netgear-router-jnr1010-version-1-0-0-24/
full-disclosure - [FD] Cross Site Request Forgery in	Exploit	MISC lists.openwall.net/full-

Netgear Router JNR1010 Version 1.0.0.24	Third Party Advisory lists.openwall.net text/html	disclosure/2016/01/11/4
Netgear 1.0.0.24 Cross Site Request Forgery ≈ Packet Storm	Exploit Third Party Advisory VDB Entry packetstormsecurity.com text/html	MISC packetstormsecurity.com/files/135215/Netgear-1.0.0.24-Cross-Site-Request-Forgery.html
Cross Site Request Forgery in Netgear Router JNR1010 Version 1.0.0.24 · Issue #13 · cybersecurityworks/Disclosed · GitHub	Exploit Third Party Advisory github.com text/html	MISC github.com/cybersecurityworks/Disclosed/issues/13
CVE-2016-11015 - Cross-Site Request Forgery in Netgear Router	Exploit Third Party Advisory cybersecurityworks.com text/html	MISC cybersecurityworks.com/zerodays/cve-2016-11015-netgear.html

There are currently no QIDs associated with this CVE

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Hardware	Netgear	Jnr1010	-	All	All	All
Hardware	Netgear	Jnr1010	-	All	All	All
Operating System	Netgear	Jnr1010 Firmware	All	All	All	All
Operating System	Netgear	Jnr1010 Firmware	All	All	All	All

cpe:2.3:h:netgear:jnr1010:-:*:*:*:*:*:*:*:

cpe:2.3:h:netgear:jnr1010:-:*:*:*:*:*:*:*:

cpe:2.3:o:netgear:jnr1010_firmware:*:*:*:*:*:*:*:*:

cpe:2.3:o:netgear:jnr1010_firmware:*:*:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→

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