



# CVE-2016-11055

[MITRE](#)[NVD](#)[CVE.ORG](#)[Print: PDF](#)

## Summary

<b>CVE</b>	CVE-2016-11055
<b>State</b>	PUBLIC
<b>Assigner</b>	cve@mitre.org
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2020-04-28 16:15:00 UTC
<b>Updated</b>	2020-05-05 19:26:00 UTC
<b>Description</b>	Certain NETGEAR devices are affected by CSRF. This affects CM400 before 2017-01-11, CM600 before 2017-01-11, D15

## Risk And Classification

**Problem Types:** CWE-352

## NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Hardware	<a href="#">Netgear</a>	<a href="#">Cm400</a>	-	All	All	All
Hardware	<a href="#">Netgear</a>	<a href="#">Cm400</a>	-	All	All	All
Operating System	<a href="#">Netgear</a>	<a href="#">Cm400 Firmware</a>	All	All	All	All
Operating System	<a href="#">Netgear</a>	<a href="#">Cm400 Firmware</a>	All	All	All	All
Hardware	<a href="#">Netgear</a>	<a href="#">Cm600</a>	-	All	All	All
Hardware	<a href="#">Netgear</a>	<a href="#">Cm600</a>	-	All	All	All
Operating System	<a href="#">Netgear</a>	<a href="#">Cm600 Firmware</a>	All	All	All	All
Operating System	<a href="#">Netgear</a>	<a href="#">Cm600 Firmware</a>	All	All	All	All
Hardware	<a href="#">Netgear</a>	<a href="#">D1500</a>	-	All	All	All
Hardware	<a href="#">Netgear</a>	<a href="#">D1500</a>	-	All	All	All
Operating System	<a href="#">Netgear</a>	<a href="#">D1500 Firmware</a>	All	All	All	All
Operating System	<a href="#">Netgear</a>	<a href="#">D1500 Firmware</a>	All	All	All	All
Hardware	<a href="#">Netgear</a>	<a href="#">D500</a>	-	All	All	All
Hardware	<a href="#">Netgear</a>	<a href="#">D500</a>	-	All	All	All
Operating System	<a href="#">Netgear</a>	<a href="#">D500 Firmware</a>	All	All	All	All
Operating System	<a href="#">Netgear</a>	<a href="#">D500 Firmware</a>	All	All	All	All
Hardware	<a href="#">Netgear</a>	<a href="#">Dst6501</a>	-	All	All	All

Hardware	<a href="#">Netgear</a>	<a href="#">Dst6501</a>	-	All	All	All
Operating System	<a href="#">Netgear</a>	<a href="#">Dst6501 Firmware</a>	All	All	All	All
Operating System	<a href="#">Netgear</a>	<a href="#">Dst6501 Firmware</a>	All	All	All	All
Hardware	<a href="#">Netgear</a>	<a href="#">Jnr1010</a>	v1	All	All	All
Hardware	<a href="#">Netgear</a>	<a href="#">Jnr1010</a>	v1	All	All	All
Operating System	<a href="#">Netgear</a>	<a href="#">Jnr1010 Firmware</a>	All	All	All	All
Operating System	<a href="#">Netgear</a>	<a href="#">Jnr1010 Firmware</a>	All	All	All	All
Hardware	<a href="#">Netgear</a>	<a href="#">Jwnr2000t</a>	v3	All	All	All
Hardware	<a href="#">Netgear</a>	<a href="#">Jwnr2000t</a>	v3	All	All	All
Operating System	<a href="#">Netgear</a>	<a href="#">Jwnr2000t Firmware</a>	All	All	All	All
Operating System	<a href="#">Netgear</a>	<a href="#">Jwnr2000t Firmware</a>	All	All	All	All
Hardware	<a href="#">Netgear</a>	<a href="#">Jwnr2010</a>	v3	All	All	All
Hardware	<a href="#">Netgear</a>	<a href="#">Jwnr2010</a>	v3	All	All	All
Operating System	<a href="#">Netgear</a>	<a href="#">Jwnr2010 Firmware</a>	All	All	All	All
Operating System	<a href="#">Netgear</a>	<a href="#">Jwnr2010 Firmware</a>	All	All	All	All
Hardware	<a href="#">Netgear</a>	<a href="#">N450 Cg3000d</a>	v2	All	All	All
Hardware	<a href="#">Netgear</a>	<a href="#">N450 Cg3000d</a>	v2	All	All	All
Operating System	<a href="#">Netgear</a>	<a href="#">N450 Cg3000d Firmware</a>	All	All	All	All
Operating System	<a href="#">Netgear</a>	<a href="#">N450 Cg3000d Firmware</a>	All	All	All	All
Hardware	<a href="#">Netgear</a>	<a href="#">Plw1000</a>	-	All	All	All
Hardware	<a href="#">Netgear</a>	<a href="#">Plw1000</a>	-	All	All	All
Operating System	<a href="#">Netgear</a>	<a href="#">Plw1000 Firmware</a>	All	All	All	All
Operating System	<a href="#">Netgear</a>	<a href="#">Plw1000 Firmware</a>	All	All	All	All
Hardware	<a href="#">Netgear</a>	<a href="#">Plw1010</a>	-	All	All	All
Hardware	<a href="#">Netgear</a>	<a href="#">Plw1010</a>	-	All	All	All
Operating System	<a href="#">Netgear</a>	<a href="#">Plw1010 Firmware</a>	All	All	All	All
Operating System	<a href="#">Netgear</a>	<a href="#">Plw1010 Firmware</a>	All	All	All	All
Hardware	<a href="#">Netgear</a>	<a href="#">Wnr500</a>	-	All	All	All
Hardware	<a href="#">Netgear</a>	<a href="#">Wnr500</a>	-	All	All	All
Operating System	<a href="#">Netgear</a>	<a href="#">Wnr500 Firmware</a>	All	All	All	All
Operating System	<a href="#">Netgear</a>	<a href="#">Wnr500 Firmware</a>	All	All	All	All
Hardware	<a href="#">Netgear</a>	<a href="#">Wnr612</a>	v3	All	All	All
Hardware	<a href="#">Netgear</a>	<a href="#">Wnr612</a>	v3	All	All	All
Operating System	<a href="#">Netgear</a>	<a href="#">Wnr612 Firmware</a>	All	All	All	All
Operating System	<a href="#">Netgear</a>	<a href="#">Wnr612 Firmware</a>	All	All	All	All

## References

Reference	Source	Link	Tags
NETGEAR Product Vulnerability Advisory: CSRF / LocalFile / XSS   Answer   NETGEAR Support	CONFIRM	<a href="https://kb.netgear.com">kb.netgear.com</a>	Vendor Ad
CVE Program record	CVE.ORG	<a href="https://www.cve.org">www.cve.org</a>	canonical
NVD vulnerability detail	NVD	<a href="https://nvd.nist.gov">nvd.nist.gov</a>	canonical,

No vendor comments have been submitted for this CVE.

There are currently no legacy QID mappings associated with this CVE.

© [CVE.report](https://cve.report) 2026 |

Use of this information constitutes acceptance for use in an AS IS condition. There are NO warranties, implied or otherwise, with regard to this information or its use. Any use of this information is at the user's risk. It is the responsibility of user to evaluate the accuracy, completeness or usefulness of any information, opinion, advice or other content. EACH USER WILL BE SOLELY RESPONSIBLE FOR ANY consequences of his or her direct or indirect use of this web site. ALL WARRANTIES OF ANY KIND ARE EXPRESSLY DISCLAIMED. This 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](https://www.mitre.org) and the authoritative source of CVE content is [MITRE's CVE web site](https://www.mitre.org/cve). This site includes MITRE data granted under the following [license](https://www.mitre.org/licenses).

**CVE.report and Source URL Uptime Status** [status.cve.report](https://status.cve.report)