



CVE-2015-1600

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

Summary

CVE	CVE-2015-1600
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2017-08-28 19:29:00 UTC
Updated	2018-10-09 19:55:00 UTC
Description	Information disclosure vulnerability in Netatmo Indoor Module firmware 100 and earlier.

Risk And Classification

Problem Types: CWE-200

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Hardware	Netatmo	Indoor Module	-	All	All	All
Hardware	Netatmo	Indoor Module	-	All	All	All
Operating System	Netatmo	Indoor Module Firmware	All	All	All	All

References

Reference	Source
Netatmo Weather Station CVE-2015-1600 Information Disclosure Vulnerability	BID
SecurityFocus	BUGT
Netatmo Weather Station Cleartext Password Leak ≈ Packet Storm	MISC
Did You Remove That Debug Code? Netatmo Weather Station Sending WPA Passphrase in the Clear - SANS Internet Storm Center	MISC
CVE Program record	CVE.C
NVD vulnerability detail	NVD

No vendor comments have been submitted for this CVE.

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

© [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](#) and the authoritative source of CVE content is [MITRE's CVE web site](#). This site includes MITRE data granted under the following [license](#).

Free CVE JSON API [cve.report/api](#)

CVE.report and Source URL Uptime Status [status.cve.report](#)