



CVE-2017-9654

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

Summary

CVE	CVE-2017-9654
State	PUBLIC
Assigner	ics-cert@hq.dhs.gov
Source Priority	CVE Program / NVD first with legacy fallback
Published	2018-04-24 15:29:00 UTC
Updated	2019-10-09 23:30:00 UTC
Description	The Philips DoseWise Portal web-based application versions 1.1.7.333 and 2.1.1.3069 stores login credentials in clear text

Risk And Classification

Problem Types: CWE-522

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Philips	Dosewise	1.1.7.333	All	All	All
Application	Philips	Dosewise	2.1.1.3069	All	All	All
Application	Philips	Dosewise	1.1.7.333	All	All	All
Application	Philips	Dosewise	2.1.1.3069	All	All	All

References

Reference	Source	Link
Philips' DoseWise Portal Vulnerabilities ICS-CERT	MISC	ics-cert.us-cert.gov
Product Security Philips	CONFIRM	www.philips.com
Philips DoseWise Portal ICSMA-17-229-01 Security Bypass and Information Disclosure Vulnerabilities	BID	www.securityfocus.com
CVE Program record	CVE.ORG	www.cve.org
NVD vulnerability detail	NVD	nvd.nist.gov

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](#).

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