



CVE-2016-10125

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

Summary

CVE	CVE-2016-10125
State	PUBLISHED
Assigner	mitre
Source Priority	CVE Program / NVD first with legacy fallback
Published	2017-01-09 17:59:00 UTC
Updated	2026-05-06 22:30:45 UTC
Description	D-Link DGS-1100 devices with Rev.B firmware 1.01.018 have a hardcoded SSL private key, which allows man-in-the-middle

Risk And Classification

Primary CVSS: v3.0 8.1 HIGH from nvd@nist.gov

CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H

EPSS: 0.007670000 probability, percentile 0.735500000 (date 2026-05-11)

Problem Types: CWE-798 | n/a

Version	Source	Type	Score	Severity	Vector
3.0	nvd@nist.gov	Primary	8.1	HIGH	CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H
2.0	nvd@nist.gov	Primary	6.8		AV:N/AC:M/Au:N/C:P/I:P/A:P

CVSS v3.0 Breakdown

Attack Vector

Network

Attack Complexity

High

Privileges Required

None

User Interaction

None

Scope

Unchanged

Confidentiality

High

Integrity

High

High

Availability

High

CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H

CVSS v2.0 Breakdown

Access Vector

Network

Access Complexity

Medium

Authentication

None

Confidentiality

Partial

Integrity

Partial

Availability

Partial

AV:N/AC:M/Au:N/C:P/I:P/A:P

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Hardware	Dlink	Dgs-1100-05	-	All	All	All
Hardware	Dlink	Dgs-1100-05pd	-	All	All	All
Hardware	Dlink	Dgs-1100-08	-	All	All	All
Hardware	Dlink	Dgs-1100-08p	-	All	All	All
Hardware	Dlink	Dgs-1100-10mp	-	All	All	All
Hardware	Dlink	Dgs-1100-10mpp	-	All	All	All
Hardware	Dlink	Dgs-1100-16	-	All	All	All
Hardware	Dlink	Dgs-1100-18	-	All	All	All
Hardware	Dlink	Dgs-1100-24	-	All	All	All
Hardware	Dlink	Dgs-1100-24p	-	All	All	All
Hardware	Dlink	Dgs-1100-26	-	All	All	All
Hardware	Dlink	Dgs-1100-26mp	-	All	All	All
Operating System	Dlink	Dgs-1100 Firmware	1.01.018	All	All	All

Vendor Declared Affected Products

Source	Vendor	Product	Version	Platforms
--------	--------	---------	---------	-----------

CNA	Na	N/a	affected n/a	Not specified
References				
Reference			Source	
DLink DGS-1100 Switch CVE-2016-10125 Local Hardcoded SSL Certificate Vulnerability			af854a3a-2127-422b-91ae-3	
CVE-2016-10125 - DLink DGS-1100 switch static hard-coded TLS crypto keys in firmware INTEGRITY Labs			af854a3a-2127-422b-91ae-3	
CVE Program record			CVE.ORG	
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](#)