



# CVE-2013-1602

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

## Summary

<b>CVE</b>	CVE-2013-1602
<b>State</b>	PUBLIC
<b>Assigner</b>	cve@mitre.org
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2020-01-28 22:15:00 UTC
<b>Updated</b>	2021-04-26 16:36:00 UTC
<b>Description</b>	An Information Disclosure vulnerability exists due to insufficient validation of authentication cookies for the RTSP session in

## Risk And Classification

**Problem Types:** CWE-200

## NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Hardware	<a href="#">Dlink</a>	<a href="#">Dcs-1100</a>	-	All	All	All
Hardware	<a href="#">Dlink</a>	<a href="#">Dcs-1100</a>	-	All	All	All
Hardware	<a href="#">Dlink</a>	<a href="#">Dcs-1100I</a>	-	All	All	All
Hardware	<a href="#">Dlink</a>	<a href="#">Dcs-1100I</a>	-	All	All	All
Operating System	<a href="#">Dlink</a>	<a href="#">Dcs-1100I Firmware</a>	1.04	All	All	All
Operating System	<a href="#">Dlink</a>	<a href="#">Dcs-1100I Firmware</a>	1.04	All	All	All
Operating System	<a href="#">Dlink</a>	<a href="#">Dcs-1100 Firmware</a>	1.03	All	All	All
Operating System	<a href="#">Dlink</a>	<a href="#">Dcs-1100 Firmware</a>	1.04	All	All	All
Operating System	<a href="#">Dlink</a>	<a href="#">Dcs-1100 Firmware</a>	1.03	All	All	All
Operating System	<a href="#">Dlink</a>	<a href="#">Dcs-1100 Firmware</a>	1.04	All	All	All
Hardware	<a href="#">Dlink</a>	<a href="#">Dcs-1130</a>	-	All	All	All
Hardware	<a href="#">Dlink</a>	<a href="#">Dcs-1130</a>	-	All	All	All
Hardware	<a href="#">Dlink</a>	<a href="#">Dcs-1130I</a>	-	All	All	All
Hardware	<a href="#">Dlink</a>	<a href="#">Dcs-1130I</a>	-	All	All	All
Operating System	<a href="#">Dlink</a>	<a href="#">Dcs-1130I Firmware</a>	1.04	All	All	All
Operating System	<a href="#">Dlink</a>	<a href="#">Dcs-1130I Firmware</a>	1.04	All	All	All
Operating System	<a href="#">Dlink</a>	<a href="#">Dcs-1130 Firmware</a>	1.03	All	All	All

Operating System	<a href="#">Dlink</a>	<a href="#">Dcs-1130 Firmware</a>	1.04	All	All	All
Operating System	<a href="#">Dlink</a>	<a href="#">Dcs-1130 Firmware</a>	1.03	All	All	All
Operating System	<a href="#">Dlink</a>	<a href="#">Dcs-1130 Firmware</a>	1.04	All	All	All
Hardware	<a href="#">Dlink</a>	<a href="#">Dcs-2102</a>	-	All	All	All
Hardware	<a href="#">Dlink</a>	<a href="#">Dcs-2102</a>	-	All	All	All
Operating System	<a href="#">Dlink</a>	<a href="#">Dcs-2102 Firmware</a>	1.05	All	All	All
Operating System	<a href="#">Dlink</a>	<a href="#">Dcs-2102 Firmware</a>	1.06	All	All	All
Operating System	<a href="#">Dlink</a>	<a href="#">Dcs-2102 Firmware</a>	1.05	All	All	All
Hardware	<a href="#">Dlink</a>	<a href="#">Dcs-2121</a>	-	All	All	All
Hardware	<a href="#">Dlink</a>	<a href="#">Dcs-2121</a>	-	All	All	All
Operating System	<a href="#">Dlink</a>	<a href="#">Dcs-2121 Firmware</a>	1.05	All	All	All
Operating System	<a href="#">Dlink</a>	<a href="#">Dcs-2121 Firmware</a>	1.06	All	All	All
Operating System	<a href="#">Dlink</a>	<a href="#">Dcs-2121 Firmware</a>	1.05	All	All	All
Hardware	<a href="#">Dlink</a>	<a href="#">Dcs-3410</a>	-	All	All	All
Hardware	<a href="#">Dlink</a>	<a href="#">Dcs-3410</a>	-	All	All	All
Operating System	<a href="#">Dlink</a>	<a href="#">Dcs-3410 Firmware</a>	1.02	All	All	All
Operating System	<a href="#">Dlink</a>	<a href="#">Dcs-3410 Firmware</a>	1.02	All	All	All
Hardware	<a href="#">Dlink</a>	<a href="#">Dcs-3411</a>	-	All	All	All
Hardware	<a href="#">Dlink</a>	<a href="#">Dcs-3411</a>	-	All	All	All
Operating System	<a href="#">Dlink</a>	<a href="#">Dcs-3411 Firmware</a>	1.02	All	All	All
Operating System	<a href="#">Dlink</a>	<a href="#">Dcs-3411 Firmware</a>	1.02	All	All	All
Hardware	<a href="#">Dlink</a>	<a href="#">Dcs-3430</a>	-	All	All	All
Hardware	<a href="#">Dlink</a>	<a href="#">Dcs-3430</a>	-	All	All	All
Operating System	<a href="#">Dlink</a>	<a href="#">Dcs-3430 Firmware</a>	1.02	All	All	All
Operating System	<a href="#">Dlink</a>	<a href="#">Dcs-3430 Firmware</a>	1.02	All	All	All
Hardware	<a href="#">Dlink</a>	<a href="#">Dcs-5230</a>	-	All	All	All
Hardware	<a href="#">Dlink</a>	<a href="#">Dcs-5230</a>	-	All	All	All
Hardware	<a href="#">Dlink</a>	<a href="#">Dcs-5230I</a>	-	All	All	All
Hardware	<a href="#">Dlink</a>	<a href="#">Dcs-5230I</a>	-	All	All	All
Operating System	<a href="#">Dlink</a>	<a href="#">Dcs-5230I Firmware</a>	1.02	All	All	All
Operating System	<a href="#">Dlink</a>	<a href="#">Dcs-5230I Firmware</a>	1.02	All	All	All
Operating System	<a href="#">Dlink</a>	<a href="#">Dcs-5230 Firmware</a>	1.02	All	All	All
Operating System	<a href="#">Dlink</a>	<a href="#">Dcs-5230 Firmware</a>	1.02	All	All	All
Hardware	<a href="#">Dlink</a>	<a href="#">Dcs-5605</a>	-	All	All	All
Hardware	<a href="#">Dlink</a>	<a href="#">Dcs-5605</a>	-	All	All	All

Operating System	<a href="#">Dlink</a>	<a href="#">Dcs-5605 Firmware</a>	1.01	All	All	All
Operating System	<a href="#">Dlink</a>	<a href="#">Dcs-5605 Firmware</a>	1.01	All	All	All
Hardware	<a href="#">Dlink</a>	<a href="#">Dcs-5635</a>	-	All	All	All
Hardware	<a href="#">Dlink</a>	<a href="#">Dcs-5635</a>	-	All	All	All
Operating System	<a href="#">Dlink</a>	<a href="#">Dcs-5635 Firmware</a>	1.01	All	All	All
Operating System	<a href="#">Dlink</a>	<a href="#">Dcs-5635 Firmware</a>	1.01	All	All	All
Hardware	<a href="#">Dlink</a>	<a href="#">Dcs-6410</a>	-	All	All	All
Hardware	<a href="#">Dlink</a>	<a href="#">Dcs-6410</a>	-	All	All	All
Operating System	<a href="#">Dlink</a>	<a href="#">Dcs-6410 Firmware</a>	1.00	All	All	All
Operating System	<a href="#">Dlink</a>	<a href="#">Dcs-6410 Firmware</a>	1.00	All	All	All
Hardware	<a href="#">Dlink</a>	<a href="#">Dcs-7410</a>	-	All	All	All
Hardware	<a href="#">Dlink</a>	<a href="#">Dcs-7410</a>	-	All	All	All
Operating System	<a href="#">Dlink</a>	<a href="#">Dcs-7410 Firmware</a>	1.00	All	All	All
Operating System	<a href="#">Dlink</a>	<a href="#">Dcs-7410 Firmware</a>	1.00	All	All	All
Hardware	<a href="#">Dlink</a>	<a href="#">Dcs-7510</a>	-	All	All	All
Hardware	<a href="#">Dlink</a>	<a href="#">Dcs-7510</a>	-	All	All	All
Operating System	<a href="#">Dlink</a>	<a href="#">Dcs-7510 Firmware</a>	1.00	All	All	All
Operating System	<a href="#">Dlink</a>	<a href="#">Dcs-7510 Firmware</a>	1.00	All	All	All
Hardware	<a href="#">Dlink</a>	<a href="#">Wcs-1100</a>	-	All	All	All
Hardware	<a href="#">Dlink</a>	<a href="#">Wcs-1100</a>	-	All	All	All
Operating System	<a href="#">Dlink</a>	<a href="#">Wcs-1100 Firmware</a>	1.00	All	All	All
Operating System	<a href="#">Dlink</a>	<a href="#">Wcs-1100 Firmware</a>	1.02	All	All	All
Operating System	<a href="#">Dlink</a>	<a href="#">Wcs-1100 Firmware</a>	1.02	All	All	All

## References

Reference	Source	Link	Tags
CVE-2013-1602 ≈ Packet Storm	MISC	<a href="http://packetstormsecurity.com">packetstormsecurity.com</a>	Third Party Ad
Multiple D-Link Products CVE-2013-1602 Information Disclosure Vulnerability	MISC	<a href="http://www.securityfocus.com">www.securityfocus.com</a>	Third Party Ad
IBM X-Force Exchange	MISC	<a href="http://exchange.xforce.ibmcloud.com">exchange.xforce.ibmcloud.com</a>	Third Party Ad
D-Link IP Cameras Multiple Vulnerabilities   CORE Security	MISC	<a href="http://www.coresecurity.com">www.coresecurity.com</a>	Exploit, Third F
CVE Program record	CVE.ORG	<a href="http://www.cve.org">www.cve.org</a>	canonical
NVD vulnerability detail	NVD	<a href="http://nvd.nist.gov">nvd.nist.gov</a>	canonical, ana

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](#)**