



CVE-2013-6811

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

Summary

CVE	CVE-2013-6811
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2019-11-22 18:15:00 UTC
Updated	2019-12-04 14:51:00 UTC
Description	Multiple cross-site request forgery (CSRF) vulnerabilities in the D-Link DSL-6740U gateway (Rev. H1) allow remote attackers to execute arbitrary code and cause a denial of service (crash) via crafted HTTP requests to the web management interface.

Risk And Classification

Problem Types: CWE-352

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Hardware	D-link	Dsl6740u	h1	All	All	All
Hardware	D-link	Dsl6740u	h1	All	All	All
Application	D-link	Dsl6740u Firmware	-	All	All	All
Application	D-link	Dsl6740u Firmware	-	All	All	All

References

Reference	Source	Link	Tags
D-Link Technical Support	MISC	web.archive.org	Third Party Advisory
IBM X-Force Exchange	MISC	exchange.xforce.ibmcloud.com	Third Party Advisory, VDB Entry
CVE Program record	CVE.ORG	www.cve.org	canonical
NVD vulnerability detail	NVD	nvd.nist.gov	canonical, analysis

No vendor comments have been submitted for this CVE.

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

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](#)