



# CVE-2014-0337

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

## Summary

<b>CVE</b>	CVE-2014-0337
<b>State</b>	PUBLIC
<b>Assigner</b>	cert@cert.org
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2014-04-05 04:01:00 UTC
<b>Updated</b>	2014-04-07 14:36:00 UTC
<b>Description</b>	Cross-site scripting (XSS) vulnerability in the web interface on Huawei Echo Life HG8247 routers with software before V100

## Risk And Classification

**Problem Types:** CWE-79

## NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Hardware	Huawei	Echo Life	hg8247	All	All	All
Hardware	Huawei	Echo Life	hg8247	All	All	All
Operating System	Huawei	Echo Life Hg8247 Firmware	v1r006c00s120	All	All	All
Operating System	Huawei	Echo Life Hg8247 Firmware	v1r006c00s120	All	All	All

## References

Reference	Source	Link	Tags
Vulnerability Note VU#917700 - Huawei Echo Life HG8247 optical router XSS vulnerability	CERT-VN	<a href="http://www.kb.cert.org">www.kb.cert.org</a>	US Government
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, analy

No vendor comments have been submitted for this CVE.

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

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](#)**