



# CVE-2013-1905

[MITRE](#)[NVD](#)[CVE.ORG](#)[JSON API](#)[Print: PDF !\[\]\(003082e50e3009141f59bd5df831749f\_img.jpg\)](#)

## Summary

<b>CVE</b>	CVE-2013-1905
<b>State</b>	PUBLIC
<b>Assigner</b>	secalert@redhat.com
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2013-06-20 23:55:00 UTC
<b>Updated</b>	2017-08-29 01:33:00 UTC
<b>Description</b>	Cross-site scripting (XSS) vulnerability in the Zero Point theme 7.x-1.x before 7.x-1.9 for Drupal allows remote attackers to i

## Risk And Classification

### Problem Types: CWE-79

## NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Catalin Florian Radut	Zeropoint	7.x-1.0	All	All	All
Application	Catalin Florian Radut	Zeropoint	7.x-1.1	All	All	All
Application	Catalin Florian Radut	Zeropoint	7.x-1.2	All	All	All
Application	Catalin Florian Radut	Zeropoint	7.x-1.3	All	All	All
Application	Catalin Florian Radut	Zeropoint	7.x-1.4	All	All	All
Application	Catalin Florian Radut	Zeropoint	7.x-1.5	All	All	All
Application	Catalin Florian Radut	Zeropoint	7.x-1.6	All	All	All
Application	Catalin Florian Radut	Zeropoint	7.x-1.7	All	All	All
Application	Catalin Florian Radut	Zeropoint	7.x-1.8	All	All	All
Application	Catalin Florian Radut	Zeropoint	7.x-1.x	dev	All	All
Application	Catalin Florian Radut	Zeropoint	7.x-1.0	All	All	All
Application	Catalin Florian Radut	Zeropoint	7.x-1.1	All	All	All
Application	Catalin Florian Radut	Zeropoint	7.x-1.2	All	All	All
Application	Catalin Florian Radut	Zeropoint	7.x-1.3	All	All	All
Application	Catalin Florian Radut	Zeropoint	7.x-1.4	All	All	All
Application	Catalin Florian Radut	Zeropoint	7.x-1.5	All	All	All
Application	Catalin Florian Radut	Zeropoint	7.x-1.6	All	All	All

Application	<a href="#">Catalin Florian Radut</a>	<a href="#">Zeropoint</a>	7.x-1.7	All	All	All
Application	<a href="#">Catalin Florian Radut</a>	<a href="#">Zeropoint</a>	7.x-1.8	All	All	All
Application	<a href="#">Catalin Florian Radut</a>	<a href="#">Zeropoint</a>	7.x-1.x	dev	All	All
Application	<a href="#">Drupal</a>	<a href="#">Drupal</a>	-	All	All	All
Application	<a href="#">Drupal</a>	<a href="#">Drupal</a>	-	All	All	All

## References

Reference	Source	Link
Drupal Zero Point 7.x Cross Site Scripting ≈ Packet Storm	MISC	<a href="https://packetstormsecurity.com">packetstormsecurity.com</a>
Full Disclosure: [Security-news] SA-CONTRIB-2013-036 - Zero Point - Cross Site Scripting (XSS)	FULLDISC	<a href="https://seclists.org">seclists.org</a>
SA-CONTRIB-2013-036 - Zero Point - Cross Site Scripting (XSS)   drupal.org	MISC	<a href="https://drupal.org">drupal.org</a>
Drupal Zero Point Module Unspecified Cross Site Scripting Vulnerability	BID	<a href="https://www.securityfocus.com">www.securityfocus.com</a>
zeropoint 7.x-1.9   drupal.org	CONFIRM	<a href="https://drupal.org">drupal.org</a>
Security Advisory SA52775 - Drupal Zero Point Theme Cross-Site Scripting Vulnerability - Secunia	SECUNIA	<a href="https://secunia.com">secunia.com</a>
IBM X-Force Exchange	XF	<a href="https://exchange.xforce.ibmcloud.com">exchange.xforce.ibmcloud.com</a>
91745	OSVDB	<a href="https://osvdb.org">osvdb.org</a>
CVE Program record	CVE.ORG	<a href="https://www.cve.org">www.cve.org</a>
NVD vulnerability detail	NVD	<a href="https://nvd.nist.gov">nvd.nist.gov</a>

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](https://cve.report/api)

CVE.report and Source URL Uptime Status [status.cve.report](https://status.cve.report)