



# CVE-2014-7280

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

## Summary

<b>CVE</b>	CVE-2014-7280
<b>State</b>	PUBLIC
<b>Assigner</b>	cve@mitre.org
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2014-10-21 15:55:00 UTC
<b>Updated</b>	2015-09-08 18:20:00 UTC
<b>Description</b>	Cross-site scripting (XSS) vulnerability in the Web UI before 2.3.4 Build #85 for Tenable Nessus 5.x allows remote web ser

## Risk And Classification

**Problem Types:** CWE-79

## NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Tenable	Web Ui	All	All	All	All

## References

Reference	Source	Link	Tags
Nessus Web UI 2.3.3 Cross Site Scripting ~ Packet Storm	MISC	<a href="http://packetstormsecurity.com">packetstormsecurity.com</a>	Exploi
112728	OSVDB	<a href="http://osvdb.org">osvdb.org</a>	
Nessus Web UI 2.3.3: Stored XSS   www.thesecurityfactory.be	MISC	<a href="http://www.thesecurityfactory.be">www.thesecurityfactory.be</a>	Exploi
Nessus Web UI 2.3.3 - Stored XSS	EXPLOIT-DB	<a href="http://www.exploit-db.com">www.exploit-db.com</a>	Exploi
Nessus Web UI CVE-2014-7280 HTML Injection Vulnerability	BID	<a href="http://www.securityfocus.com">www.securityfocus.com</a>	Exploi
[R1] Tenable Nessus Web UI Scanned Content Stored XSS   Tenable Network Security	CONFIRM	<a href="http://www.tenable.com">www.tenable.com</a>	Vendc
Full Disclosure: Nessus Web UI 2.3.3: Stored XSS	FULLDISC	<a href="http://seclists.org">seclists.org</a>	Exploi
CVE Program record	CVE.ORG	<a href="http://www.cve.org">www.cve.org</a>	canon
NVD vulnerability detail	NVD	<a href="http://nvd.nist.gov">nvd.nist.gov</a>	canon

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](#)**