



# CVE-2014-4980

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

## Summary

<b>CVE</b>	CVE-2014-4980
<b>State</b>	PUBLIC
<b>Assigner</b>	cve@mitre.org
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2014-07-23 14:55:00 UTC
<b>Updated</b>	2018-10-09 19:49:00 UTC
<b>Description</b>	The /server/properties resource in Tenable Web UI before 2.3.5 for Nessus 5.2.3 through 5.2.7 allows remote attackers to c

## Risk And Classification

**Problem Types:** CWE-200

## NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Tenable	Nessus	5.2.3	All	All	All
Application	Tenable	Nessus	5.2.4	All	All	All
Application	Tenable	Nessus	5.2.5	All	All	All
Application	Tenable	Nessus	5.2.6	All	All	All
Application	Tenable	Nessus	5.2.7	All	All	All
Application	Tenable	Nessus	5.2.3	All	All	All
Application	Tenable	Nessus	5.2.4	All	All	All
Application	Tenable	Nessus	5.2.5	All	All	All
Application	Tenable	Nessus	5.2.6	All	All	All
Application	Tenable	Nessus	5.2.7	All	All	All
Application	Tenable	Web Ui	All	All	All	All

## References

Reference	Source
[R4] Tenable Nessus Web UI /server/properties token Parameter Remote Information Disclosure   Tenable Network Security	CONFIRM
109376	OSVDB
SecurityFocus	BUGTRAQ

Tenable Nessus 5.2.7 Parameter Tampering / Authentication Bypass ≈ Packet Storm	MISC
Nessus Web UI CVE-2014-4980 Information Disclosure Vulnerability	BID
CVE-2014-4980 Parameter Tampering in Nessus Web UI	MISC
Tenable Nessus Access Control Flaw in Web UI Lets Remote Users Obtain Potentially Sensitive Information - SecurityTracker	SECTRACK
CVE Program record	CVE.ORG
NVD vulnerability detail	NVD



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](#)**