



# CVE-2014-2605

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

## Summary

<b>CVE</b>	CVE-2014-2605
<b>State</b>	PUBLIC
<b>Assigner</b>	hp-security-alert@hp.com
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2014-07-16 04:58:00 UTC
<b>Updated</b>	2017-08-29 01:34:00 UTC
<b>Description</b>	Unspecified vulnerability in HP StoreVirtual 4000 Storage and StoreVirtual VSA 9.5 through 11.0 allows remote attackers to

## Risk And Classification

**Problem Types:** NVD-CWE-noinfo

## NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	<a href="#">Hp</a>	<a href="#">Storage Management Software</a>	10.0	All	All	All
Application	<a href="#">Hp</a>	<a href="#">Storage Management Software</a>	10.5	All	All	All
Application	<a href="#">Hp</a>	<a href="#">Storage Management Software</a>	11.0	All	All	All
Application	<a href="#">Hp</a>	<a href="#">Storage Management Software</a>	9.5	All	All	All
Application	<a href="#">Hp</a>	<a href="#">Storage Management Software</a>	10.0	All	All	All
Application	<a href="#">Hp</a>	<a href="#">Storage Management Software</a>	10.5	All	All	All
Application	<a href="#">Hp</a>	<a href="#">Storage Management Software</a>	11.0	All	All	All
Application	<a href="#">Hp</a>	<a href="#">Storage Management Software</a>	9.5	All	All	All
Hardware	<a href="#">Hp</a>	<a href="#">Storevirtual 4130</a>	-	All	All	All
Hardware	<a href="#">Hp</a>	<a href="#">Storevirtual 4130</a>	-	All	All	All
Hardware	<a href="#">Hp</a>	<a href="#">Storevirtual 4330</a>	-	All	All	All
Hardware	<a href="#">Hp</a>	<a href="#">Storevirtual 4330</a>	-	All	All	All
Hardware	<a href="#">Hp</a>	<a href="#">Storevirtual 4330fc</a>	-	All	All	All
Hardware	<a href="#">Hp</a>	<a href="#">Storevirtual 4330fc</a>	-	All	All	All
Hardware	<a href="#">Hp</a>	<a href="#">Storevirtual 4335</a>	-	All	All	All
Hardware	<a href="#">Hp</a>	<a href="#">Storevirtual 4335</a>	-	All	All	All
Hardware	<a href="#">Hp</a>	<a href="#">Storevirtual 4530</a>	-	All	All	All

Hardware	<a href="#">Hp</a>	<a href="#">Storevirtual 4530</a>	-	All	All	All
Hardware	<a href="#">Hp</a>	<a href="#">Storevirtual 4630</a>	-	All	All	All
Hardware	<a href="#">Hp</a>	<a href="#">Storevirtual 4630</a>	-	All	All	All
Hardware	<a href="#">Hp</a>	<a href="#">Storevirtual 4730</a>	-	All	All	All
Hardware	<a href="#">Hp</a>	<a href="#">Storevirtual 4730</a>	-	All	All	All
Hardware	<a href="#">Hp</a>	<a href="#">Storevirtual 4730fc</a>	-	All	All	All
Hardware	<a href="#">Hp</a>	<a href="#">Storevirtual 4730fc</a>	-	All	All	All
Application	<a href="#">Hp</a>	<a href="#">Storevirtual Vsa</a>	-	All	All	All
Application	<a href="#">Hp</a>	<a href="#">Storevirtual Vsa</a>	-	All	All	All

## References

Reference	Score
IBM X-Force Exchange	XF
HP StoreVirtual Bugs Let Remote Users Obtain Information and Remote Authenticated Users Gain Elevated Privileges - SecurityTracker	SE
Software and Drivers	HI
HP StoreVirtual 4000 Storage and StoreVirtual VSA Unspecified Information Disclosure Vulnerability	BI
CVE Program record	CV
NVD vulnerability detail	NV

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](#)**