



CVE-2013-2352

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

Summary

CVE	CVE-2013-2352
State	PUBLIC
Assigner	hp-security-alert@hp.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2013-07-10 22:55:00 UTC
Updated	2019-10-09 23:07:00 UTC
Description	LeftHand OS (aka SAN iQ) 10.5 and earlier on HP StoreVirtual Storage devices does not provide a mechanism for disabling

Risk And Classification

Problem Types: CWE-255

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Hardware	Dell	Poweredge 2950	All	All	All	All
Hardware	Dell	Poweredge 2950	All	All	All	All
Hardware	Hp	DI320s	All	All	All	All
Hardware	Hp	DI320s	All	All	All	All
Hardware	Hp	Lefthand Nsm2060	All	All	All	All
Hardware	Hp	Lefthand Nsm2060	All	All	All	All
Hardware	Hp	Lefthand Nsm2060 G2	All	All	All	All
Hardware	Hp	Lefthand Nsm2060 G2	All	All	All	All
Hardware	Hp	Lefthand Nsm2120 G2	All	All	All	All
Hardware	Hp	Lefthand Nsm2120 G2	All	All	All	All
Hardware	Hp	Lefthand Vsa	All	All	All	All
Hardware	Hp	Lefthand Vsa	All	All	All	All
Hardware	Hp	P4000 Vsa	All	All	All	All
Hardware	Hp	P4000 Vsa	All	All	All	All
Hardware	Hp	P4300	All	All	All	All
Hardware	Hp	P4300	All	All	All	All
Hardware	Hp	P4300 G2	All	All	All	All

Hardware	Hp	P4300 G2	All	All	All	All
Hardware	Hp	P4500	All	All	All	All
Hardware	Hp	P4500	All	All	All	All
Hardware	Hp	P4500 G2	All	All	All	All
Hardware	Hp	P4500 G2	All	All	All	All
Hardware	Hp	P4900 G2	All	All	All	All
Hardware	Hp	P4900 G2	All	All	All	All
Application	Hp	San/iq	10.0	All	All	All
Application	Hp	San/iq	8.0	All	All	All
Application	Hp	San/iq	8.1	All	All	All
Application	Hp	San/iq	8.5	All	All	All
Application	Hp	San/iq	9.0	All	All	All
Application	Hp	San/iq	9.5	All	All	All
Application	Hp	San/iq	All	All	All	All
Application	Hp	San/iq	10.0	All	All	All
Application	Hp	San/iq	8.0	All	All	All
Application	Hp	San/iq	8.1	All	All	All
Application	Hp	San/iq	8.5	All	All	All
Application	Hp	San/iq	9.0	All	All	All
Application	Hp	San/iq	9.5	All	All	All
Application	Hp	San/iq	10.0	All	All	All
Application	Hp	San/iq	8.0	All	All	All
Application	Hp	San/iq	8.1	All	All	All
Application	Hp	San/iq	8.5	All	All	All
Application	Hp	San/iq	9.0	All	All	All
Application	Hp	San/iq	9.5	All	All	All
Application	Hp	San/iq	All	All	All	All
Hardware	Hp	Storevirtual 4130	All	All	All	All
Hardware	Hp	Storevirtual 4130	All	All	All	All
Hardware	Hp	Storevirtual 4330	All	All	All	All
Hardware	Hp	Storevirtual 4330	All	All	All	All
Hardware	Hp	Storevirtual 4530	All	All	All	All
Hardware	Hp	Storevirtual 4530	All	All	All	All
Hardware	Hp	Storevirtual 4630	All	All	All	All
Hardware	Hp	Storevirtual 4630	All	All	All	All

Hardware	Hp	Storevirtual 4730	All	All	All	All
Hardware	Hp	Storevirtual 4730	All	All	All	All
Hardware	Hp	Storevirtual Vsa	All	All	All	All
Hardware	Hp	Storevirtual Vsa	All	All	All	All
Hardware	Ibm	X3650	All	All	All	All
Hardware	Ibm	X3650	All	All	All	All

References

Reference	Source	Link	Tags
HP Support document - HP Support Center	HP	h20564.www2.hp.com	Vendor Advisory
HP storage: more possible backdoors • The Register	MISC	www.theregister.co.uk	
CVE Program record	CVE.ORG	www.cve.org	canonical
NVD vulnerability detail	NVD	nvd.nist.gov	canonical, analysis

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