CVE-2012-4361

MITRE | NVD | CVE.ORG | JSON API | Print: PDF

Summary

CVE	CVE-2012-4361
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2012-08-20 22:55:00 UTC
Updated	2012-08-21 04:00:00 UTC
Description	lhn/public/network/ping in HP SAN/iQ before 9.5 on the HP Virtual SAN Appliance allows remote authenticated users to exe

Risk And Classification

Problem Types: CWE-78

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
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	All	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	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	All	All	All	All
Hardware	Hp	Virtual San Appliance	-	All	All	All
Hardware	Hp	Virtual San Appliance	-	All	All	All

References

Reference	Source	Link	Ta
HP VSA Remote Command Execution Exploit	EXPLOIT-DB	www.exploit-db.com	Ex

US-CERT Vulnerability Note VU#441363 - HP Virtual SAN appliance root shell command injection	CERT-VN	www.kb.cert.org	US
HP StorageWorks P4000 Virtual SAN Appliance Command Execution	EXPLOIT-DB	www.exploit-db.com	Ex
CVE Program record	CVE.ORG	www.cve.org	ca
NVD vulnerability detail	NVD	nvd.nist.gov	ca

No vendor comments have been submitted for this CVE.

There are currently no legacy QID mappings associated with this CVE.