



# CVE-2002-0763

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

## Summary

<b>CVE</b>	CVE-2002-0763
<b>State</b>	PUBLIC
<b>Assigner</b>	cve@mitre.org
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2002-08-12 04:00:00 UTC
<b>Updated</b>	2008-09-05 20:28:00 UTC
<b>Description</b>	Vulnerability in administration server for HP VirtualVault 4.5 on HP-UX 11.04 allows remote web servers or privileged external users to execute arbitrary code on the target system.

## Risk And Classification

**Problem Types:** NVD-CWE-Other

## NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	<a href="#">Hp</a>	<a href="#">Virtualvault</a>	4.5	All	All	All
Application	<a href="#">Hp</a>	<a href="#">Virtualvault</a>	4.5	All	All	All

## References

Reference	Source
Neohapsis Archives - HP Security Digests - HP-UX security bulletins digest - From support_feedbackus-support-mail.external.hp.com	HP
HP Virtualvault Unauthorized Administrative Access Vulnerability	BID
ISS X-Force Database: hp-virtualvault-admin-access (9038): HP VirtualVault could allow unauthorized administrative access	XF
CVE Program record	CVE
NVD vulnerability detail	NVD

No vendor comments have been submitted for this CVE.

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

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](#)**