



CVE-2016-4392

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

Summary

CVE	CVE-2016-4392
State	PUBLIC
Assigner	security-alert@hpe.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2018-08-06 20:29:00 UTC
Updated	2018-10-05 16:46:00 UTC
Description	A remote cross site scripting vulnerability has been identified in HP Business Service Management software v9.1x, v9.20 - v

Risk And Classification

Problem Types: CWE-79

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Hp	Business Service Management	9.10	All	All	All
Application	Hp	Business Service Management	9.25	ip1	All	All
Application	Hp	Business Service Management	9.10	All	All	All
Application	Hp	Business Service Management	9.25	ip1	All	All
Application	Hp	Business Service Management	All	All	All	All

References

Reference	Sour
HP Business Service Management CVE-2016-4392 Cross Site Scripting Vulnerability	BID
HPE Business Service Management Input Validation Flaw Lets Remote Users Conduct Cross-Site Scripting Attacks - SecurityTracker	SEC
Document Display HPE Support Center	CON
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.

© [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](#).

Free CVE JSON API [cve.report/api](#)

CVE.report and Source URL Uptime Status [status.cve.report](#)