



CVE-2011-1863

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

Summary

CVE	CVE-2011-1863
State	PUBLISHED
Assigner	hp
Source Priority	CVE Program / NVD first with legacy fallback
Published	2011-06-14 17:55:04 UTC
Updated	2026-04-29 01:13:23 UTC
Description	HP Service Manager 7.02, 7.11, 9.20, and 9.21 and Service Center 6.2.8 allow remote authenticated users to conduct unsop

Risk And Classification

Primary CVSS: v2.0 7.5 from nvd@nist.gov

AV:N/AC:M/Au:S/C:C/I:P/A:P

Problem Types: CWE-94 | n/a

CVSS v2.0 Breakdown

Access Vector

Network

Access Complexity

Medium

Authentication

Single

Confidentiality

Complete

Integrity

Partial

Availability

Partial

AV:N/AC:M/Au:S/C:C/I:P/A:P

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Hp	Service Center	6.2.8	All	All	All

Application	Hp	Service Manager	7.02	All	All	All
Application	Hp	Service Manager	7.11	All	All	All
Application	Hp	Service Manager	9.20	All	All	All
Application	Hp	Service Manager	9.21	All	All	All

Vendor Declared Affected Products						
Source	Vendor	Product	Version	Platforms		
CNA	Na	N/a	affected n/a	Not specified		

References						
Reference						
'[security bulletin] HPSBMA02674 SSRT100487 rev.1 - HP Service Manager and HP Service Center, Unautho' - MARC						
HP Service Manager and Service Center Multiple Vulnerabilities - Secunia.com						
HP Service Manager and Service Center Multiple Vulnerabilities						
IBM X-Force Exchange						
HP Service Manager and HP Service Center Multiple Vulns - SecurityReason.com						
HP Service Manager Multiple Bugs Let Remote Authenticated Users Gain Access and Inject Scripting Code, Remote Users Conduct Cross-Si						
CVE Program record						
NVD vulnerability detail						

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](#)