CVE-2012-2561

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

Summary

CVE	CVE-2012-2561
State	PUBLISHED
Assigner	certcc
Source Priority	CVE Program / NVD first with legacy fallback
Published	2012-05-21 20:55:21 UTC
Updated	2026-04-29 01:13:23 UTC
Description	HP Business Service Management (BSM) 9.12 does not properly restrict the uploading of .war files, which allows remote at

Risk And Classification

Primary CVSS: v2.0 10 from nvd@nist.gov

AV:N/AC:L/Au:N/C:C/I:C/A:C

Problem Types: CWE-264 | n/a

CVSS v2.0 Breakdown

Access Vector

Network

Access Complexity

Low

Authentication

None

Confidentiality

Complete

Integrity

Complete

Availability

Complete

AV:N/AC:L/Au:N/C:C/I:C/A:C

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Hp	Business Service Management	9.12	All	All	All

Vendor Declared Affected Products

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

References

Reference	Source
osvdb.org/81981	af854a3a-21
HP Business Service Management Default JBOSS Configuration Lets Remote Users Execute Arbitrary Code - SecurityTracker	af854a3a-21
Security Advisory SA49218 - HP Business Service Management WAR Deployment Code Execution Vulnerability - Secunia	af854a3a-21
Vulnerability Note VU#859230 - HP Business Service Management 9.12 remote code execution vulnerability	af854a3a-21
HP Business Service Management CVE-2012-2561 Remote Code Execution Vulnerability	af854a3a-21
'[security bulletin] HPSBMU02792 SSRT100820 rev.1 - HP Business Service Management (BSM), Remote Unau' - MARC	af854a3a-21
CVE Program record	CVE.ORG
NVD vulnerability detail	NVD

No vendor comments have been submitted for this CVE.

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