



CVE-2008-0495

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

Summary

CVE	CVE-2008-0495
State	PUBLISHED
Assigner	mitre
Source Priority	CVE Program / NVD first with legacy fallback
Published	2008-01-30 22:00:00 UTC
Updated	2026-04-23 00:35:47 UTC
Description	Unspecified vulnerability in the Pegasus CIM Server in IBM Hardware Management Console (HMC) 7 R3.2.0 allows remote

Risk And Classification

Primary CVSS: v2.0 7.8 from nvd@nist.gov

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

Problem Types: NVD-CWE-noinfo | n/a

CVSS v2.0 Breakdown

Access Vector

Network

Access Complexity

Low

Authentication

None

Confidentiality

None

Integrity

None

Availability

Complete

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

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	ibm	Hardware Management Console	7.3.2.0	All	All	All

Vendor Declared Affected Products				
Source	Vendor	Product	Version	Platforms
CNA	Na	N/a	affected n/a	Not specified
References				
Reference				Source
IBM AIX Pegasus CIM Server for Director Vulnerabilities - Advisories - Secunia				af854a
Webmail - OVH				af854a
Webmail - OVH				af854a
IBM Hardware Management Console Pegasus CIM Server Denial Of Service Vulnerability				af854a
IBM X-Force Exchange				af854a
IBM notice: The page you requested cannot be displayed				af854a
IBM Hardware Management Console Pegasus CIM Denial of Service - Secunia Advisories - Vulnerability Intelligence - Secunia.com				af854a
www14.software.ibm.com/webapp/set2/subscriptions/pqvcmd				af854a
SecurityTracker.com Archives - IBM Hardware Management Console Pegasus CIM Bug Lets Remote Users Deny Service				af854a
IBM Support: Fix Central				af854a
CVE Program record				CVE.C
NVD vulnerability detail				NVD
Vendor Comments And Credit				
Organization	Published	Contributor	Statement	
Red Hat	2008-02-08	Mark J Cox	We believe this issue is a duplicate of CVE-2007-5360. Not vulnerable. This issue did not affect	
There are currently no legacy QID mappings associated with this CVE.				