



CVE-2009-3900

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

Summary

CVE	CVE-2009-3900
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2009-11-06 15:30:00 UTC
Updated	2017-08-17 01:31:00 UTC
Description	Unspecified vulnerability in the Cluster Management component in IBM PowerHA 5.4, 5.4.1, 5.5, and 6.1 on AIX allows remote attackers to execute arbitrary code or cause a denial of service (DoS) via a crafted request.

Risk And Classification

Problem Types: NVD-CWE-noinfo

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Ibm	Aix	All	All	All	All
Operating System	Ibm	Aix	All	All	All	All
Application	Ibm	Powerha	5.4	All	All	All
Application	Ibm	Powerha	5.4.1	All	All	All
Application	Ibm	Powerha	5.5	All	All	All
Application	Ibm	Powerha	6.1	All	All	All
Application	Ibm	Powerha	5.4	All	All	All
Application	Ibm	Powerha	5.4.1	All	All	All
Application	Ibm	Powerha	5.5	All	All	All
Application	Ibm	Powerha	6.1	All	All	All

References

Reference	Source	Link	Tags
IBM notice: The page you requested cannot be displayed	AIXAPAR	www-01.ibm.com	
aix.software.ibm.com/aix/efixes/security/haport_advisory.asc	CONFIRM	aix.software.ibm.com	Exploit
IBM AIX PowerHA Cluster Management Data Manipulation - Secunia.com	SECUNIA	secunia.com	Vendor Advisory
Webmail : Solution de messagerie professionnelle - OVHcloud- OVH	VUPEN	www.vupen.com	Patch, Vendor Ad

IBM PowerHA Cluster Management Unauthorized Access Vulnerability	BID	www.securityfocus.com	Patch
IBM X-Force Exchange	XF	exchange.xforce.ibmcloud.com	
IBM notice: The page you requested cannot be displayed	AIXAPAR	www-01.ibm.com	
IBM notice: The page you requested cannot be displayed	AIXAPAR	www-01.ibm.com	Vendor Advisory
CVE Program record	CVE.ORG	www.cve.org	canonical
NVD vulnerability detail	NVD	nvd.nist.gov	canonical, analysi



No vendor comments have been submitted for this CVE.

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