CVE-2013-4810

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

Summary

CVE	CVE-2013-4810
State	PUBLISHED
Assigner	hp
Source Priority	CVE Program / NVD first with legacy fallback
Published	2013-09-16 13:01:46 UTC
Updated	2026-04-21 19:12:54 UTC
Description	HP ProCurve Manager (PCM) 3.20 and 4.0, PCM+ 3.20 and 4.0, Identity Driven Manager (IDM) 4.0, and Application Lifecy

Risk And Classification

Primary CVSS: v3.1 9.8 CRITICAL from nvd@nist.gov

CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H

EPSS: 0.896950000 probability, percentile 0.995680000 (date 2026-04-25)

CISA KEV: Listed on 2022-03-25; due 2022-04-15; ransomware use Unknown

Problem Types: CWE-94 | n/a | CWE-94 CWE-94 Improper Control of Generation of Code ('Code Injection')

Version	Source	Type	Score	Severity	Vector
3.1	nvd@nist.gov	Primary	9.8	CRITICAL	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H
3.1	ADP	DECLARED	9.8	CRITICAL	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H
3.1	134c704f-9b21-4f2e-91b3-4a467353bcc0	Secondary	9.8	CRITICAL	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H
2.0	nvd@nist.gov	Primary	10		AV:N/AC:L/Au:N/C:C/I:C/A:C

CVSS v3.1 Breakdown

Attack Vector

Network

Attack Complexity

Low

Privileges Required

None

User Interaction

None

Scope

Unchanged

Confidentiality

High

Integrity

High

Availability

High

CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H

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

CISA Known Exploited Vulnerability

Vendor	Hewlett Packard (HP)
Product	ProCurve Manager (PCM), PCM+, Identity Driven Manager (IDM), and Application Lifecycle Management
Name	HP Multiple Products Remote Code Execution Vulnerability
Required Action	Apply updates per vendor instructions.
Notes	https://nvd.nist.gov/vuln/detail/CVE-2013-4810

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Hp	Application Lifecycle Management	-	All	All	All
Application	Hp	Procurve Manager	3.20	All	All	All
Application	Hp	Procurve Manager	3.20	All	All	All
Application	Hp	Procurve Manager	4.0	All	All	All

Application	Hp	Procurve Manager	4.0	All	All	All

Vendor Declared Affected Products

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

References

Reference	Source
'[security bulletin] HPSBGN02952 rev.1 - HP Application Lifecycle Manager (ALM) Running JBoss Applica' - MARC	af854a3a-2
About Secunia Research | Flexera	af854a3a-2
Zero Day Initiative	af854a3a-2
Apache Tomcat/JBoss EJBInvokerServlet / JMXInvokerServlet (RMI over HTTP) Marshalled Object RCE	af854a3a-2
www.cisa.gov/known-exploited-vulnerabilities-catalog	134c704f-9
'[security bulletin] HPSBGN03323 rev.1 - HP Business Service Automation Essentials Core with JBOSS, R' - MARC	af854a3a-2
Documento de soporte HP - Centro de Soporte de HP	af854a3a-2
HP ProCurve Manager Bugs Let Remote Users Inject SQL Commands, Hijack Sessions, and Code Execution - SecurityTracker	af854a3a-2
CVE Program record	CVE.ORG
NVD vulnerability detail	NVD
CISA Known Exploited Vulnerabilities catalog	CISA

No vendor comments have been submitted for this CVE.

Additional Advisory Data

Source	Time	Event
ADP	2022-03-25T00:00:00.000Z	CVE-2013-4810 added to CISA KEV

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