

CVE-2013-4810

Hewlett Packard (HP) HP Multiple Products Remote Code Execution Vulnerability

CISA KEV since Mar 25, 2022

Actively exploited

HP ProCurve Manager (PCM) 3.20 and 4.0, PCM+ 3.20 and 4.0, Identity Driven Manager (IDM) 4.0, and Application Lifecycle Management allow remote attackers to execute arbitrary code via a marshalled object to (1) EJInvokerServlet or (2) JMXInvokerServlet, aka ZDI-CAN-1760. NOTE: this is probably a duplicate of CVE-2007-1036, CVE-2010-0738, and/or CVE-2012-0874.

EVRS 82/100 Urgent priority	CVSS V3.1 9.8 Critical · NVD	EPSS 0.795 99.61st percentile · FIRST	CISA DEADLINE Apr 15, 2022 KEV since 2022 · listed over a year
--	--	---	--

Signals behind the score

☒ counted in the score ☐ not counted

evidence for 6 of 8 signals

☒ CISA KEV	Listed in the catalog	☐ Vendor exploitation	Confirmed exploitation in the wild
☐ Ransomware	No known ransomware campaign association	☐ KEV recency	On the CISA KEV catalog for over two years
☒ EPSS	0.795 probability	☐ Pre-patch disclosure	Disclosure status unavailable
☒ CVSS	Base score 9.8	☐ Microsoft Exploitability Index	Not a Microsoft CVE

Remediation

Patch This Cycle Patch or fixed version identified

CISA required action: Apply updates per vendor instructions.

Basis: CISA KEV required action

Affected and fixed versions

PACKAGE	AFFECTED	FIXED IN	SOURCE
application lifecycle management	—	no fixed version listed	NVD
procurve manager	3.20 4.0	no fixed version listed	NVD

Sources

Vendor guidance	github.com/advisories/GHSA-mm58-72w4-25hp	NVD	nvd.nist.gov/vuln/detail/CVE-2013-4810
CISA KEV	cisa.gov/known-exploited-vulnerabilities-catalog	ENISA EUVD	euvd.enisa.europa.eu/vulnerability/EUVD-2013-4655
Current data	evulnable.com/vulnerability-management/cve/CVE-2013-4810		

Snapshot at generation time. EPSS can move quickly. A public exploit module is not evidence of active exploitation.