HCL BigFix Service Management (SM) Discovery is vulnerable to unenforced encryption

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

Summary

CVE	CVE-2025-31981
State	PUBLISHED
Assigner	HCL
Source Priority	CVE Program / NVD first with legacy fallback
Published	2026-04-21 15:16:35 UTC
Updated	2026-04-22 15:09:37 UTC
Description	HCL BigFix Service Management (SM) Discovery is vulnerable to unenforced encryption due to port 80 (HTTP) being open

Risk And Classification

Primary CVSS: v3.1 5.3 MEDIUM from psirt@hcl.com

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

EPSS: 0.000110000 probability, percentile 0.014060000 (date 2026-04-22)

Problem Types: CWE-319 | CWE-319 CWE-319 Cleartext transmission of sensitive information

Version	Source	Type	Score	Severity	Vector
3.1	psirt@hcl.com	Secondary	5.3	MEDIUM	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N
3.1	CNA	CVSS	5.3	MEDIUM	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N

CVSS v3.1 Breakdown

Attack Vector

Network

Attack Complexity

Low

Privileges Required

None

User Interaction

None

Scope

Unchanged

Confidentiality

Low

ntegrity

None

Availability

None

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

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Hcltech	Bigfix Service Management	23.0	All	All	All

Vendor Declared Affected Products

Source	Vendor	Product	Version	Platforms
CNA	HCLSoftware	BigFix Service Management SM	affected 23	Not specified

References

Reference	Source	Link	Tags
support.hcl-software.com/csm	psirt@hcl.com	support.hcl-software.com	Vendor Advisory
CVE Program record	CVE.ORG	www.cve.org	canonical
NVD vulnerability detail	NVD	nvd.nist.gov	canonical, analysis

No vendor comments have been submitted for this CVE.

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

© CVE.report 2026 |
Use of this information constitutes acceptance for use in an AS IS condition. There are NO warranties, implied or otherwise, with regard to this information or its use. Any use of this information is at the user's risk. It is the responsibility of user to evaluate the accuracy, completeness or usefulness of any information, opinion, advice or other content. EACH USER WILL BE SOLELY RESPONSIBLE FOR ANY consequences of his or her direct or indirect use of this web site. ALL WARRANTIES OF ANY KIND ARE EXPRESSLY DISCLAIMED. This site will NOT BE LIABLE FOR ANY DIRECT, INDIRECT or any other kind of loss.

CVE, CWE, and OVAL are registred trademarks of The MITRE Corporation and the authoritative source of CVE content is MITRE's CVE web site. This site includes MITRE data granted under the following license.

Free CVE JSON API cve.report/api

CVE.report and Source URL Uptime Status **status.cve.report**