CVE-2016-2948

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

Summary

CVE	CVE-2016-2948
State	PUBLISHED
Assigner	ibm
Source Priority	CVE Program / NVD first with legacy fallback
Published	2016-11-30 11:59:11 UTC
Updated	2026-05-06 22:30:45 UTC
Description	IBM BigFix Remote Control before 9.1.3 allows local users to discover hardcoded credentials via unspecified vectors.

Risk And Classification

Primary CVSS: v3.0 7.8 HIGH from nvd@nist.gov

CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H

EPSS: 0.000470000 probability, percentile 0.146460000 (date 2026-05-09)

Problem Types: CWE-798 | n/a

Version	Source	Type	Score	Severity	Vector
3.0	nvd@nist.gov	Primary	7.8	HIGH	CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H
2.0	nvd@nist.gov	Primary	4.6		AV:L/AC:L/Au:N/C:P/I:P/A:P

CVSS v3.0 Breakdown

Attack Vector
Local

Attack Complexity
Low

Privileges Required
Low

User Interaction
None

Scope
Unchanged

Confidentiality
High

Integrity
High

Availability

High

CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H

CVSS v2.0 Breakdown

Access Vector

Local

Access Complexity

Low

Authentication

None

Confidentiality

Partial

Integrity

Partial

Availability

Partial

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

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Ibm	Bigfix Remote Control	9.1.2	All	All	All

Vendor Declared Affected Products

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

References

Reference
IBM IV89781: SECURITY APAR CVE-2016-2948 HARD CODED CREDENTIALS USED IN IBM BIGFIX REMOTE CONTROL - United States
IBM Security Bulletin: Hard coded credentials used in IBM BigFix Remote Control (CVE-2016-2948) - United States
IBM BigFix Remote Control CVE-2016-2948 Local Information Disclosure Vulnerability
CVE Program record
NVD vulnerability detail

No vendor comments have been submitted for this CVE.

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

Free CVE JSON API cve.report/api

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