IBM Maximo Application Suite was vulnerable to because Cookie ltpatoken2_<workspace_name> was not set with secure flag

MITRE | NVD | CVE.ORG | Print: PDF

Summary

CVE	CVE-2026-4820
State	PUBLISHED
Assigner	ibm
Source Priority	CVE Program / NVD first with legacy fallback
Published	2026-04-01 21:17:02 UTC
Updated	2026-04-01 21:17:02 UTC
Description	IBM Maximo Application Suite 9.1, 9.0, 8.11, and 8.10 does not set the secure attribute on authorization tokens or session c

Risk And Classification

Primary CVSS: v3.1 4.3 MEDIUM from psirt@us.ibm.com

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

Problem Types: CWE-614 | CWE-614 CWE-614 Sensitive Cookie in HTTPS Session Without 'Secure' Attribute

Version	Source	Type	Score	Severity	Vector
3.1	psirt@us.ibm.com	Primary	4.3	MEDIUM	CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:L/I:N/A:N
3.1	CNA	CVSS	4.3	MEDIUM	CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:L/I:N/A:N

CVSS v3.1 Breakdown

Attack Vector

Network

Attack Complexity

Low

Privileges Required

None

User Interaction

Required

Scope

Unchanged

Confidentiality

Low

ntegrity

None

Availability

None

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

Vendor Declared Affected Products

Source	Vendor	Product	Version	Platforms
CNA	IBM	Maximo Application Suite	affected 9.1.0 10.6.5.0 semver	Not specified
CNA	IBM	Maximo Application Suite	affected 9.0 semver	Not specified
CNA	IBM	Maximo Application Suite	affected 8.11.0 semver	Not specified
CNA	IBM	Maximo Application Suite	affected 8.10 semver	Not specified

References

Reference	Source	Link	Tags
www.ibm.com/support/pages/node/7268028	psirt@us.ibm.com	www.ibm.com	
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.

Additional Advisory Data

Solutions

CNA: Remediated Product(s)Version(s)IBM Maximo Application Suite9.1.8IBM Maximo Application Suite9.0.19IBM Maximo Application Suite8.11.30IBM Maximo Application Suite8.10.33

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