CVE-2016-5004

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

Summary

CVE	CVE-2016-5004
State	PUBLISHED
Assigner	redhat
Source Priority	CVE Program / NVD first with legacy fallback
Published	2017-06-06 18:29:00 UTC
Updated	2025-04-20 01:37:25 UTC
Description	The Content-Encoding HTTP header feature in ws-xmlrpc 3.1.3 as used in Apache Archiva allows remote attackers to caus

Risk And Classification

Primary CVSS: v3.0 6.5 MEDIUM from nvd@nist.gov

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

Problem Types: CWE-400 | n/a

Version	Source	Type	Score	Severity	Vector
3.0	nvd@nist.gov	Primary	6.5	MEDIUM	CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:N/I:N/A:H
2.0	nvd@nist.gov	Primary	4.3		AV:N/AC:M/Au:N/C:N/I:N/A:P

CVSS v3.0 Breakdown

Attack Vector

Network

Attack Complexity

Low

Privileges Required

None

User Interaction

Required

Scope

Unchanged

Confidentiality

None

Integrity

None

Availability

High

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

CVSS v2.0 Breakdown

Access Vector

Network

Access Complexity

Medium

Authentication

None

Confidentiality

None

Integrity

None

Availability

Partial

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

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Apache	Ws-xmlrpc	3.1.3	All	All	All

Vendor Declared Affected Products

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

References

Reference
oss-security - Vulnerabilities in Apache Archiva
GitHub - 0ang3el/unsafe-xmlrpc
Apache Archiva Bugs in XML-RPC Library Let Remote Users Conduct Server-Side Request Forgery Attacks, Deny Service, and Potentially Ex
Malformed Request
Beware of ws-xmlrpc library in your Java App ~ Из крайности в безопасность
CVE Program record
NVD vulnerability detail

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

994949 Java (Maven) Security Update for org.apache.xmlrpc:xmlrpc-common (GHSA-r2pg-w96p-pcpj)

Free CVE JSON API cve.report/api

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