CVE-2017-12149

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

Summary

CVE	CVE-2017-12149
State	PUBLISHED
Assigner	redhat
Source Priority	CVE Program / NVD first with legacy fallback
Published	2017-10-04 21:01:00 UTC
Updated	2026-04-21 19:36:59 UTC
Description	In Jboss Application Server as shipped with Red Hat Enterprise Application Platform 5.2, it was found that the doFilter meth

Risk And Classification

Primary CVSS: v3.1 9.8 CRITICAL from nvd@nist.gov

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

EPSS: 0.942940000 probability, percentile 0.999450000 (date 2026-05-03)

CISA KEV: Listed on 2021-12-10; due 2022-06-10; ransomware use Known

Problem Types: CWE-502 | CWE-502 CWE-502 | CWE-502 CWE-502 Deserialization of Untrusted Data

Version	Source	Type	Score	Severity	Vector
3.1	nvd@nist.gov	Primary	9.8	CRITICAL	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H
3.1	ADP	DECLARED	9.8	CRITICAL	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H
3.1	134c704f-9b21-4f2e-91b3-4a467353bcc0	Secondary	9.8	CRITICAL	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H
2.0	nvd@nist.gov	Primary	7.5		AV:N/AC:L/Au:N/C:P/I:P/A:P

CVSS v3.1 Breakdown

Attack Vector

Network

Attack Complexity

Low

Privileges Required

None

User Interaction

None

Scope

Unchanged

Confidentiality

High

Integrity

High

Availability

High

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

CVSS v2.0 Breakdown

Access Vector

Network

Access Complexity

Low

Authentication

None

Confidentiality

Partial

Integrity

Partial

Availability

Partial

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

CISA Known Exploited Vulnerability

Vendor	Red Hat
Product	JBoss Application Server
Name	Red Hat JBoss Application Server Remote Code Execution Vulnerability
Required Action	Apply updates per vendor instructions.
Notes	https://nvd.nist.gov/vuln/detail/CVE-2017-12149

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Redhat	Jboss Enterprise Application Platform	-	All	All	All
Application	Redhat	Jboss Enterprise Application Platform	5.0.0	All	All	All
Application	Redhat	Jboss Enterprise Application Platform	5.0.1	All	All	All
Application	Redhat	Jboss Enterprise Application Platform	5.1.0	All	All	All
Application	Redhat	Jboss Enterprise Application Platform	5.1.1	All	All	All

Application	Redhat	Jboss Enterprise Application Platform	5.1.2	All	All	All
Application	Redhat	Jboss Enterprise Application Platform	5.2.0	All	All	All
Application	Redhat	Jboss Enterprise Application Platform	5.2.1	All	All	All
Application	Redhat	Jboss Enterprise Application Platform	5.2.2	All	All	All

Vendor Declared Affected Products

Source	Vendor	Product	Version	Platforms
CNA	Red Hat Inc.	Jbossas	affected n/a	Not specified

References

Reference
Red Hat Customer Portal
Red Hat Jboss Enterprise Application Platform CVE-2017-12149 Remote Code Execution Vulnerability
Exploits/CVE-2017-12149 at master · gottburgm/Exploits · GitHub
Bug 1486220 – CVE-2017-12149 jbossas: Arbitrary code execution via unrestricted deserialization in ReadOnlyAccessFilter of HTTP Invoker.
www.cisa.gov/known-exploited-vulnerabilities-catalog
Red Hat Customer Portal
CVE Program record
NVD vulnerability detail
CISA Known Exploited Vulnerabilities catalog

No vendor comments have been submitted for this CVE.

Additional Advisory Data

Source	Time	Event
ADP	2021-12-10T00:00:00.000Z	CVE-2017-12149 added to CISA KEV

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**