Org.hibernate/hibernate-core: hibernate: information disclosure and data deletion via second-order sql injection

MITRE | NVD | CVE.ORG | Print: PDF

Summary

CVE	CVE-2026-0603
State	PUBLISHED
Assigner	redhat
Source Priority	CVE Program / NVD first with legacy fallback
Published	2026-01-23 07:15:53 UTC
Updated	2026-03-30 12:16:26 UTC
Description	A flaw was found in Hibernate. A remote attacker with low privileges could exploit a second-order SQL injection vulnerabilit

Risk And Classification

Primary CVSS: v3.1 8.3 HIGH from secalert@redhat.com

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

EPSS: 0.000590000 probability, percentile 0.185430000 (date 2026-04-02)

Problem Types: CWE-89 | CWE-89 Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')

Version	Source	Type	Score	Severity	Vector
3.1	secalert@redhat.com	Secondary	8.3	HIGH	CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:L
3.1	CNA	CVSS	8.3	HIGH	CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:L

CVSS v3.1 Breakdown

Attack Vector

Network

Attack Complexity

Low

Privileges Required

Low

User Interaction

None

Scope

Unchanged

Confidentiality

High

Integrity

High

Availability

Low

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

Vendor Declared Affected Products

Source	Vendor	Product	Version
CNA	Red Hat	Red Hat JBoss Enterprise Application Platform 7.1 EUS For RHEL 7	unaffected 0:5.1.17-4.Final_redhat_00005.1.ep7.
CNA	Red Hat	Red Hat JBoss Enterprise Application Platform 7.1 EUS For RHEL 7	unaffected 0:7.1.14-4.GA_redhat_00003.1.ep7.el
CNA	Red Hat	Red Hat JBoss Enterprise Application Platform 7.3 EUS For RHEL 7	unaffected 0:5.3.38-1.Final_redhat_00001.1.el7ea
CNA	Red Hat	Red Hat JBoss Enterprise Application Platform 7.3 EUS For RHEL 7	unaffected 0:7.3.17-5.GA_redhat_00006.1.el7eap
CNA	Red Hat	Red Hat JBoss Enterprise Application Platform 7.4	Not specified
CNA	Red Hat	Red Hat JBoss Enterprise Application Platform 7.4 ELS On RHEL 7	unaffected 0:5.3.38-1.Final_redhat_00001.1.el7ea
CNA	Red Hat	Red Hat JBoss Enterprise Application Platform 7.4 ELS On RHEL 7	unaffected 0:7.4.24-4.GA_redhat_00002.1.el7eap
CNA	Red Hat	Red Hat JBoss Enterprise Application Platform 7.4 ELS On RHEL 8	unaffected 0:5.3.38-1.Final_redhat_00001.1.el8ea
CNA	Red Hat	Red Hat JBoss Enterprise Application Platform 7.4 ELS On RHEL 8	unaffected 0:7.4.24-4.GA_redhat_00002.1.el8eap
CNA	Red Hat	Red Hat JBoss Enterprise Application Platform 7.4 ELS On RHEL 9	unaffected 0:5.3.38-1.Final_redhat_00001.1.el9ea
CNA	Red Hat	Red Hat JBoss Enterprise Application Platform 7.4 ELS On RHEL 9	unaffected 0:7.4.24-4.GA_redhat_00002.1.el9eap
CNA	Red Hat	Red Hat AMQ Broker 7	Not specified
CNA	Red Hat	Red Hat Build Of OptaPlanner 8	Not specified
CNA	Red Hat	Red Hat Data Grid 8	Not specified
CNA	Red Hat	Red Hat Fuse 7	Not specified
CNA	Red Hat	Red Hat JBoss Enterprise Application Platform 8	Not specified
CNA	Red Hat	Red Hat JBoss Enterprise Application Platform Expansion Pack	Not specified
CNA	Red Hat	Red Hat OpenShift AI RHOAI	Not specified
CNA	Red Hat	Red Hat OpenShift AI RHOAI	Not specified
CNA	Red Hat	Red Hat OpenShift Dev Spaces	Not specified
CNA	Red Hat	Red Hat OpenShift Dev Spaces	Not specified
CNA	Red Hat	Red Hat Process Automation 7	Not specified
CNA	Red Hat	Red Hat Satellite 6	Not specified
CNA	Red Hat	Red Hat Satellite 6	Not specified
CNA	Red Hat	Red Hat Single Sign-On 7	Not specified

References

Reference	Source	Link	Tags
access.redhat.com/errata/RHSA-2026:6011	secalert@redhat.com	access.redhat.com	
access.redhat.com/errata/RHSA-2026:4924	secalert@redhat.com	access.redhat.com	
access.redhat.com/errata/RHSA-2026:6012	secalert@redhat.com	access.redhat.com	
access.redhat.com/errata/RHSA-2026:4916	secalert@redhat.com	access.redhat.com	
bugzilla.redhat.com/show_bug.cgi	secalert@redhat.com	bugzilla.redhat.com	
access.redhat.com/security/cve/CVE-2026-0603	secalert@redhat.com	access.redhat.com	
access.redhat.com/errata/RHSA-2026:4915	secalert@redhat.com	access.redhat.com	
access.redhat.com/errata/RHSA-2026:4917	secalert@redhat.com	access.redhat.com	
CVE Program record	CVE.ORG	www.cve.org	canonical
NVD vulnerability detail	NVD	nvd.nist.gov	canonical, analysis

Vendor Comments And Credit

Discovery Credit

CNA: Red Hat would like to thank Christiaan Swiers (YouGina) and Tommy Williams (HeroDevs) for reporting this issue. (en)

Additional Advisory Data

Source	Time	Event
CNA	2026-01-05T13:12:29.816Z	Reported to Red Hat.
CNA	2026-01-19T10:10:00.000Z	Made public.

Workarounds

CNA: Mitigation for this issue is either not available or the currently available options do not meet the Red Hat Product Security criteria comprising ease of use and deployment, applicability to widespread installation base or stability.

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