Rhdh: graphql injection leading to platform-wide denial of service (dos) in rh developer hub orchestrator plugin

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

Summary

CVE	CVE-2026-3118
State	PUBLISHED
Assigner	redhat
Source Priority	CVE Program / NVD first with legacy fallback
Published	2026-02-25 12:16:17 UTC
Updated	2026-04-22 20:16:41 UTC
Description	A security flaw was identified in the Orchestrator Plugin of Red Hat Developer Hub (Backstage). The issue occurs due to ins

Risk And Classification

Primary CVSS: v3.1 6.5 MEDIUM from secalert@redhat.com

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

EPSS: 0.000160000 probability, percentile 0.035520000 (date 2026-04-22)

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	6.5	MEDIUM	CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H
3.1	CNA	CVSS	6.5	MEDIUM	CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H

CVSS v3.1 Breakdown

Attack Vector

Network

Attack Complexity

Low

Privileges Required

Low

User Interaction

None

Scope

Unchanged

Confidentiality

None

ntegrity

None

Availability

High

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

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Redhat	Developer Hub	-	All	All	All

Vendor Declared Affected Products

Source	Vendor	Product	Version
CNA	Red Hat	Red Hat Developer Hub 1.8	unaffected sha256:bb763e2b7a9d101f73b03b9e1c5688e7034fd9d31413e890817bd4098

References

Reference	Source	Link	Tags
access.redhat.com/errata/RHSA-2026:9742	secalert@redhat.com	access.redhat.com	
access.redhat.com/security/cve/CVE-2026-3118	secalert@redhat.com	access.redhat.com	Vendor Advisory
bugzilla.redhat.com/show_bug.cgi	secalert@redhat.com	bugzilla.redhat.com	Issue Tracking, Vendor Advisory
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 Thibault Guittet for reporting this issue. (en)

Additional Advisory Data

Source	Time	Event
CNA	2026-02-24T12:08:42.955Z	Reported to Red Hat.
CNA	2026-02-24T00:00:00.000Z	Made public.

Workarounds

CNA: To mitigate this issue, restrict network access to the Red Hat Developer Hub instance to trusted users and networks only. This limits the exposure of the vulnerable Orchestrator Plugin to unauthorized access.

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**