Cockpit: cockpit: arbitrary command execution via crafted links in system logs ui

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

Summary

CVE	CVE-2026-4802
State	PUBLISHED
Assigner	redhat
Source Priority	CVE Program / NVD first with legacy fallback
Published	2026-05-11 14:16:31 UTC
Updated	2026-05-11 14:16:31 UTC
Description	A flaw was found in Cockpit. This vulnerability allows a remote attacker to achieve arbitrary command execution on the hos

Risk And Classification

Primary CVSS: v3.1 8 HIGH from secalert@redhat.com

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

Problem Types: CWE-78 | CWE-78 Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')

Version	Source	Type	Score	Severity	Vector
3.1	secalert@redhat.com	Primary	8	HIGH	CVSS:3.1/AV:N/AC:L/PR:L/UI:R/S:U/C:H/I:H/A:H
3.1	CNA	CVSS	8	HIGH	CVSS:3.1/AV:N/AC:L/PR:L/UI:R/S:U/C:H/I:H/A:H

CVSS v3.1 Breakdown

Attack Vector
Network

Attack Complexity
Low

Privileges Required
Low

User Interaction
Required

Scope
Unchanged

Confidentiality
High

Integrity

Integrity
High
Availability
High

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

Vendor Declared Affected Products

Source	Vendor	Product	Version	Platforms
CNA	Red Hat	Red Hat Enterprise Linux 10	Not specified	Not specified
CNA	Red Hat	Red Hat Enterprise Linux 7	Not specified	Not specified
CNA	Red Hat	Red Hat Enterprise Linux 8	Not specified	Not specified
CNA	Red Hat	Red Hat Enterprise Linux 9	Not specified	Not specified

References

Reference	Source	Link	Tags
bugzilla.redhat.com/show_bug.cgi	secalert@redhat.com	bugzilla.redhat.com	
github.com/cockpit-project/cockpit/blob/e204cd130/pkg/systemd/logsJourna...	secalert@redhat.com	github.com	
access.redhat.com/security/cve/CVE-2026-4802	secalert@redhat.com	access.redhat.com	
CVE Program record	CVE.ORG	www.cve.org	canonical
NVD vulnerability detail	NVD	nvd.nist.gov	canonical, analy

Vendor Comments And Credit

Discovery Credit

CNA: Red Hat would like to thank Gabriel Rodrigues (HAKAI) for reporting this issue. (en)

Additional Advisory Data

Source	Time	Event
CNA	2026-03-25T10:32:01.264Z	Reported to Red Hat.
CNA	2026-05-11T12:34:26.148Z	Made public.

Workarounds

CNA: Mitigation for this issue is either not available or the currently available options don't meet the Red Hat Product Security criteria comprising ease of use and deployment, applicability to widespread installation base or stability. Operational risk reduction until fixes are available: restrict access to Cockpit to trusted networks/users only, and avoid opening untrusted crafted Cockpit URLs

There are currently no legacy OID mappings associated with this CVE

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

Free CVE JSON API cve.report/api

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