Aap-controller: aap-gateway: account hijacking and unauthorized access via unverified email linking

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

Summary

CVE	CVE-2026-6266
State	PUBLISHED
Assigner	redhat
Source Priority	CVE Program / NVD first with legacy fallback
Published	2026-05-04 14:16:35 UTC
Updated	2026-05-04 22:16:19 UTC
Description	A flaw was found in the AAP gateway. The user auto-link strategy, introduced in AAP 2.6, automatically links an external Ide

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: 0.000420000 probability, percentile 0.126210000 (date 2026-05-05)

Problem Types: CWE-305 | CWE-305 Authentication Bypass by Primary Weakness

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

ntegrity

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	Platforms
CNA	Red Hat	Red Hat Ansible Automation Platform 2.5 For RHEL 8	unaffected 0:4.6.28-3.el8ap * rpm	Not specified
CNA	Red Hat	Red Hat Ansible Automation Platform 2.5 For RHEL 8	unaffected 0:2.5.20260422-2.el8ap * rpm	Not specified
CNA	Red Hat	Red Hat Ansible Automation Platform 2.5 For RHEL 8	unaffected 0:2.5.20260422-2.el8ap * rpm	Not specified
CNA	Red Hat	Red Hat Ansible Automation Platform 2.5 For RHEL 9	unaffected 0:4.6.28-3.el9ap * rpm	Not specified
CNA	Red Hat	Red Hat Ansible Automation Platform 2.5 For RHEL 9	unaffected 0:2.5.20260422-2.el9ap * rpm	Not specified
CNA	Red Hat	Red Hat Ansible Automation Platform 2.5 For RHEL 9	unaffected 0:2.5.20260422-2.el9ap * rpm	Not specified
CNA	Red Hat	Red Hat Ansible Automation Platform 2.6 For RHEL 9	unaffected 0:4.7.11-2.el9ap * rpm	Not specified
CNA	Red Hat	Red Hat Ansible Automation Platform 2.6 For RHEL 9	unaffected 0:2.6.20260422-1.el9ap * rpm	Not specified
CNA	Red Hat	Red Hat Ansible Automation Platform 2.6 For RHEL 9	unaffected 0:2.6.20260422-1.el9ap * rpm	Not specified
CNA	Red Hat	Red Hat Ansible Automation Platform 2.6	unaffected 1777377014 * rpm	Not specified
CNA	Red Hat	Red Hat Ansible Automation Platform 2.6	unaffected 1777311120 * rpm	Not specified

References

Reference	Source	Link	Tags
access.redhat.com/errata/RHSA-2026:13545	secalert@redhat.com	access.redhat.com	
access.redhat.com/security/cve/CVE-2026-6266	secalert@redhat.com	access.redhat.com	
access.redhat.com/errata/RHSA-2026:13512	secalert@redhat.com	access.redhat.com	
access.redhat.com/errata/RHSA-2026:13508	secalert@redhat.com	access.redhat.com	
bugzilla.redhat.com/show_bug.cgi	secalert@redhat.com	bugzilla.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: This issue was discovered by Robin Bobbitt (Red Hat). (en)

Additional Advisory Data

Source	Time	Event

CNA	2026-04-14T06:29:16.779Z	Reported to Red Hat.
CNA	2026-05-04T13:35:24.113Z	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.