Bug 2458142 (CVE-2026-6266) - CVE-2026-6266 aap-controller: aap-gateway: Account hijacking and unauthorized access via unverified email linking

Keywords: Security

Status: NEW

Alias: CVE-2026-6266

Product: Security Response

Component: vulnerability

Version: unspecified

Hardware: All

OS: Linux

Priority: high

Severity: high

Target Milestone: ---

Assignee: Product Security

QA Contact:

Docs Contact:

URL:

Whiteboard:

Depends On:

Blocks:

TreeView+ depends on / blocked

Reported: 2026-04-14 06:33 UTC by OSIDB Bzimport

Modified: 2026-05-04 14:16 UTC (History)

CC List: 10 users (show)

Fixed In Version:

Clone Of:

Environment:

Last Closed:

Embargoed:

Attachments	(Terms of Use)

Links

System	ID	Private	Priority	Status	Summary	Last Updated
Red Hat Product Errata	RHSA-2026:13508	0	None	None	None	2026-05-04 13:59:08 UTC
Red Hat Product Errata	RHSA-2026:13512	0	None	None	None	2026-05-04 14:16:00 UTC

OSIDB Bzimport 2026-04-14 06:33:43 UTC Description

AAP 2.6 introduced a user auto-link strategy that automatically links an external IDP identity to an existing AAP user account when the IDP-provided email matches a user's email. The system performs no verification that the email is actually proven to belong to the authenticating user, and the behavior is hard-coded with no admin toggle. This creates two primary exploitable attack paths: (1) a regular AAP user can pre-position their account to pre-hijack a victim's first IDP login; (2) an attacker who can set an arbitrary email on a configured IDP can link to any existing AAP account, including admin accounts.

errata-xmlrpc 2026-05-04 13:59:06 UTC Comment 3

This issue has been addressed in the following products:

  Red Hat Ansible Automation Platform 2.6 for RHEL 10
  Red Hat Ansible Automation Platform 2.6 for RHEL 9

Via RHSA-2026:13508 https://access.redhat.com/errata/RHSA-2026:13508

errata-xmlrpc 2026-05-04 14:15:59 UTC Comment 4

This issue has been addressed in the following products:

  Red Hat Ansible Automation Platform 2.5 for RHEL 9
  Red Hat Ansible Automation Platform 2.5 for RHEL 8

Via RHSA-2026:13512 https://access.redhat.com/errata/RHSA-2026:13512

Note

You need to log in before you can comment on or make changes to this bug.