Paperclip Vulnerable to Unauthenticated Remote Code Execution via Import Authorization Bypass

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

Summary

CVE	CVE-2026-41679
State	PUBLISHED
Assigner	GitHub_M
Source Priority	CVE Program / NVD first with legacy fallback
Published	2026-04-23 02:16:19 UTC
Updated	2026-04-23 02:16:19 UTC
Description	Paperclip is a Node.js server and React UI that orchestrates a team of AI agents to run a business. Prior to version 2026.41

Risk And Classification

Primary CVSS: v3.1 10 CRITICAL from security-advisories@github.com

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

Problem Types: CWE-287 | CWE-862 | CWE-1188 | CWE-287 CWE-287: Improper Authentication | CWE-862 CWE-862: Missing Authorization | CWE-1188 CWE-1188: Insecure Default Initialization of Resource

Version	Source	Type	Score	Severity	Vector
3.1	security-advisories@github.com	Secondary	10	CRITICAL	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:H/A:H
3.1	CNA	DECLARED	10	CRITICAL	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:H/A:H

CVSS v3.1 Breakdown

Attack Vector

Network

Attack Complexity

Low

Privileges Required

None

User Interaction

None

Scope

Changed

Confidentiality

High

ntegrity

High

Availability

High

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

Vendor Declared Affected Products

Source	Vendor	Product	Version	Platforms
CNA	Paperclipai	Paperclip	affected < 2026.410.0	Not specified
CNA	Paperclipai	@paperclipai/server	affected < 2026.410.0	Not specified

References

Reference	Source	Link	Tags
github.com/paperclipai/paperclip/security/advisories/GHSA-68qg-g8mg-6pr7	security-advisories@github.com	github.com	
CVE Program record	CVE.ORG	www.cve.org	canonical
NVD vulnerability detail	NVD	nvd.nist.gov	canonical, a

No vendor comments have been submitted for this CVE.

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