CVE-2026-6356

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

Summary

CVE	CVE-2026-6356
State	PUBLISHED
Assigner	certcc
Source Priority	CVE Program / NVD first with legacy fallback
Published	2026-04-22 14:17:06 UTC
Updated	2026-05-12 20:06:18 UTC
Description	A vulnerability in the web application allows standard users to escalate their privileges to those of a super administrator thro

Risk And Classification

Primary CVSS: v3.1 9.6 CRITICAL from ADP

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

EPSS: 0.000320000 probability, percentile 0.091910000 (date 2026-05-12)

Problem Types: CWE-1220 | CWE-1220: Insufficient Granularity of Access Control | CWE-1220 CWE-1220 Insufficient Granularity of Access Control

Version	Source	Type	Score	Severity	Vector
3.1	ADP	DECLARED	9.6	CRITICAL	CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:C/C:H/I:H/A:N
3.1	134c704f-9b21-4f2e-91b3-4a467353bcc0	Secondary	9.6	CRITICAL	CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:C/C:H/I:H/A:N

CVSS v3.1 Breakdown

Attack Vector

Network

Attack Complexity

Low

Privileges Required

Low

User Interaction

None

Scope

Changed

Confidentiality

High

ntegrity

High

Availability

None

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

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Augmentt	Augmentt	All	All	All	All

Vendor Declared Affected Products

Source	Vendor	Product	Version	Platforms
CNA	Augmentt	Augmentt	affected 1.0	Not specified

References

Reference	Source	Link	Tags
github.com/Penguinsecq/CVE-2026-6356	134c704f-9b21-4f2e-91b3-4a467353bcc0	github.com	Third Party Advisory, Mitigation
CVE Program record	CVE.ORG	www.cve.org	canonical
NVD vulnerability detail	NVD	nvd.nist.gov	canonical, analysis

No vendor comments have been submitted for this CVE.

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