CVE-2005-4856

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

Summary

CVE	CVE-2005-4856
State	PUBLISHED
Assigner	mitre
Source Priority	CVE Program / NVD first with legacy fallback
Published	2005-12-31 05:00:00 UTC
Updated	2025-04-03 01:03:51 UTC
Description	The admin interface in eZ publish 3.5 before 3.5.7, 3.6 before 3.6.5, 3.7 before 3.7.3, and 3.8 before 20051110 does not pr

Risk And Classification

Primary CVSS: v2.0 5 from nvd@nist.gov

AV:N/AC:L/Au:N/C:P/I:N/A:N

Problem Types: CWE-19 | n/a

CVSS v2.0 Breakdown

Access Vector

Network

Access Complexity

Low

Authentication

None

Confidentiality

Partial

Integrity

None

Availability

None

AV:N/AC:L/Au:N/C:P/I:N/A:N

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Ez	Ez Publish	3.5.0	All	All	All

Application	Ez	Ez Publish	3.5.1	All	All	All
Application	Ez	Ez Publish	3.5.2	All	All	All
Application	Ez	Ez Publish	3.5.3	All	All	All
Application	Ez	Ez Publish	3.5.4	All	All	All
Application	Ez	Ez Publish	3.5.5	All	All	All
Application	Ez	Ez Publish	3.5.6	All	All	All
Application	Ez	Ez Publish	3.6.0	All	All	All
Application	Ez	Ez Publish	3.6.1	All	All	All
Application	Ez	Ez Publish	3.6.2	All	All	All
Application	Ez	Ez Publish	3.6.3	All	All	All
Application	Ez	Ez Publish	3.6.4	All	All	All
Application	Ez	Ez Publish	3.7.0	All	All	All
Application	Ez	Ez Publish	3.7.1	All	All	All
Application	Ez	Ez Publish	3.7.2	All	All	All
Application	Ez	Ez Publish	All	All	All	All

Vendor Declared Affected Products

Source	Vendor	Product	Version	Platforms
CNA	Na	N/a	affected n/a	Not specified

References

Reference	Source
Page not found	af854a3a-2127-422b-91ae-36
eZ Issue Tracker: Issue #006703: Security issue with error templates on admin interface - eZ Publish Project	af854a3a-2127-422b-91ae-36
CVE Program record	CVE.ORG
NVD vulnerability detail	NVD

No vendor comments have been submitted for 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**