CVE-2007-0535

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

Summary

CVE	CVE-2007-0535
State	PUBLISHED
Assigner	mitre
Source Priority	CVE Program / NVD first with legacy fallback
Published	2007-01-26 01:28:00 UTC
Updated	2026-04-23 00:35:47 UTC
Description	Multiple eval injection vulnerabilities in Vote! Pro 4.0, and possibly earlier, allow remote attackers to execute arbitrary code

Risk And Classification

Primary CVSS: v2.0 7.5 from nvd@nist.gov

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

Problem Types: NVD-CWE-Other | n/a

CVSS v2.0 Breakdown

Access Vector

Network

Access Complexity

Low

Authentication

None

Confidentiality

Partial

Integrity

Partial

Availability

Partial

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

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Vote Pro	Vote Pro	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	Link	Tags
osvdb.org/31606	af854a3a-2127-422b-91ae-364da2661108	osvdb.org	
Webmail : Solution de messagerie professionnelle - OVHcloud- OVH	af854a3a-2127-422b-91ae-364da2661108	www.vupen.com	
Vote! Pro PHP "eval()" Injection Vulnerability - Advisories - Secunia	af854a3a-2127-422b-91ae-364da2661108	secunia.com	Vend
CVE Program record	CVE.ORG	www.cve.org	canor
NVD vulnerability detail	NVD	nvd.nist.gov	canor

No vendor comments have been submitted for this CVE.

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