CVE-2006-0484

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

Summary

CVE	CVE-2006-0484
State	PUBLISHED
Assigner	mitre
Source Priority	CVE Program / NVD first with legacy fallback
Published	2006-01-31 20:03:00 UTC
Updated	2025-04-03 01:03:51 UTC
Description	Directory traversal vulnerability in Vis.pl, as part of the FACE CONTROL product, allows remote attackers to read arbitrary f

Risk And Classification

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

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

EPSS: 0.006740000 probability, percentile 0.714680000 (date 2026-04-16)

Problem Types: NVD-CWE-Other | 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	Elido	Face Control	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
[HSC] Multiple transversal bug in vis - CXSecurity.com	af854a3a-2
SecurityFocus	af854a3a-2
SecurityTracker.com Archives - Face Control Input Validation Hole in 'vis.pl' Lets Remote Users Traverse the Directory	af854a3a-2
IBM X-Force Exchange	af854a3a-2
Elido Face Control Multiple Directory Traversal Vulnerabilities	af854a3a-2
[HSC] Multiple transversal bug in vis.pl : Hackers Center : Internet Security Archive: Exploits, Patch, Security Articles, Advisories	af854a3a-2
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.