



CVE-2001-0924

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

Summary

CVE	CVE-2001-0924
State	PUBLISHED
Assigner	mitre
Source Priority	CVE Program / NVD first with legacy fallback
Published	2001-11-22 05:00:00 UTC
Updated	2025-04-03 01:03:51 UTC
Description	Directory traversal vulnerability in ifx CGI program in Informix Web DataBlade allows remote attackers to read arbitrary files

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: 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	ibm	Informix Web Datablade	3.3	All	All	All

Application	l bm	Informix Web Datablade	3.4	All	All	All
Application	l bm	Informix Web Datablade	3.5	All	All	All
Application	l bm	Informix Web Datablade	3.6	All	All	All
Application	l bm	Informix Web Datablade	3.7	All	All	All
Application	l bm	Informix Web Datablade	4.10	All	All	All
Application	l bm	Informix Web Datablade	4.11	All	All	All
Application	l bm	Informix Web Datablade	4.12	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
IBM X-Force Exchange	af854a3a-2127-422b-91ae-364da2661108	exchange.xforce.ibm
IBM Informix Web Datablade Directory Traversal Vulnerability	af854a3a-2127-422b-91ae-364da2661108	www.securityfocus.c
'Re: double dot vulnerability on a site running Informix database.' - MARC	af854a3a-2127-422b-91ae-364da2661108	marc.info
'double dot vulnerability on a site running Informix database.' - MARC	af854a3a-2127-422b-91ae-364da2661108	marc.info
CVE Program record	CVE.ORG	www.cve.org
NVD vulnerability detail	NVD	nvd.nist.gov

No vendor comments have been submitted for this CVE.

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