CVE-2005-0115

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

Summary

CVE	CVE-2005-0115
State	PUBLISHED
Assigner	mitre
Source Priority	CVE Program / NVD first with legacy fallback
Published	2005-01-24 05:00:00 UTC
Updated	2025-04-03 01:03:51 UTC
Description	Stack-based buffer overflow in DataRescue Interactive Disassembler (IDA) Pro 4.7 allows attackers to execute arbitrary coc

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	Datarescue	Ida	4.7	All	All	All

Vendor Declared Affected Products

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

References

Reference
iDefense : Power Of Intelligence : Current Intelligence : Vulnerabilities
404 Not Found
Secunia - Advisories - IDA Pro Import Library Name Handling Buffer Overflow
IBM X-Force Exchange
SecurityTracker.com Archives - DataRescue IDA Pro PE Buffer Overflow in Import Library Name May Let Remote Users Execute Arbitrary Co
DataRescue IDA Pro Malformed PE File Remote Buffer Overflow Vulnerability
CVE Program record
NVD vulnerability detail

No vendor comments have been submitted for this CVE.

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