CVE-2014-8531

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

Summary

CVE	CVE-2014-8531
State	PUBLISHED
Assigner	mitre
Source Priority	CVE Program / NVD first with legacy fallback
Published	2014-10-29 14:55:04 UTC
Updated	2026-05-06 22:30:45 UTC
Description	The TLS/SSL Server in McAfee Network Data Loss Prevention (NDLP) before 9.3 uses weak cipher algorithms, which mak

Risk And Classification

Primary CVSS: v2.0 6.5 from nvd@nist.gov

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

Problem Types: CWE-310 | n/a

CVSS v2.0 Breakdown

Access Vector

Network

Access Complexity

Low

Authentication

Single

Confidentiality

Partial

Integrity

Partial

Availability

Partial

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

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Mcafee	Network Data Loss Prevention	8.6	All	All	All

Application	Mcafee	Network Data Loss Prevention	9.2.0	All	All	All
Application	Mcafee	Network Data Loss Prevention	9.2.1	All	All	All
Application	Mcafee	Network Data Loss Prevention	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
McAfee Network Data Loss Prevention CVE-2014-8531 Weak Encryption Algorithm Security Weakness	af854a3a-2127-422b-91
IBM X-Force Exchange	af854a3a-2127-422b-91
McAfee KnowledgeBase - McAfee Security Bulletin – Network Data Loss Prevention addresses 17 security issues	af854a3a-2127-422b-91
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.