CVE-2017-4015

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

Summary

CVE	CVE-2017-4015
State	PUBLISHED
Assigner	intel
Source Priority	CVE Program / NVD first with legacy fallback
Published	2017-05-17 21:29:00 UTC
Updated	2025-04-20 01:37:25 UTC
Description	Clickjacking vulnerability in the server in McAfee Network Data Loss Prevention (NDLP) 9.3.x allows remote authenticated u

Risk And Classification

Primary CVSS: v3.1 4.5 MEDIUM from nvd@nist.gov

CVSS:3.1/AV:N/AC:L/PR:H/UI:R/S:U/C:N/I:H/A:N

Problem Types: CWE-1021 | Clickjacking vulnerability

Version	Source	Type	Score	Severity	Vector
3.1	nvd@nist.gov	Primary	4.5	MEDIUM	CVSS:3.1/AV:N/AC:L/PR:H/UI:R/S:U/C:N/I:H/A:N
2.0	nvd@nist.gov	Primary	3.5		AV:N/AC:M/Au:S/C:N/I:P/A:N

CVSS v3.1 Breakdown

Attack Vector

Network

Attack Complexity

Low

Privileges Required

High

User Interaction

Required

Scope

Unchanged

Confidentiality

None

Integrity

High

Availability

None

CVSS:3.1/AV:N/AC:L/PR:H/UI:R/S:U/C:N/I:H/A:N

CVSS v2.0 Breakdown

Access Vector

Network

Access Complexity

Medium

Authentication

Single

Confidentiality

None

Integrity

Partial

Availability

None

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

NVD Known Affected Configurations (CPE 2.3)

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

Vendor Declared Affected Products

Source	Vendor	Product	Version	Platforms
CNA	McAfee	Network Data Loss Prevention NDLP	affected 9.3.x	Not specified

References

Reference
McAfee Network Data Loss Prevention Multiple Bugs Let Remote Users Conduct Session Hijacking and Cross-Site Scripting Attacks and Obta
McAfee Security Bulletin - Network Data Loss Prevention update fixes eleven vulnerabilities (CVE-2017-3933, CVE-2017-3934, CVE-2017-39
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.

Free CVE JSON API cve.report/api

CVE.report and Source URL Uptime Status status.cve.report