



MITRE NVD CVE.ORG JSON API Print: PDF

CVE	CVE-2017-4016
State	PUBLIC
Assigner	secure@intel.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2017-05-17 21:29:00 UTC
Updated	2017-07-08 01:29:00 UTC
Description	Web Server method disclosure in the server in McAfee Network Data Loss Prevention (NDLP) 9.3.x allows remote attacker

Problem Types: CWE-200

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

Reference
McAfee Security Bulletin - Network Data Loss Prevention update fixes eleven vulnerabilities (CVE-2017-3933, CVE-2017-3934, CVE-2017-3935, CVE-2017-3936, CVE-2017-3937, CVE-2017-3938, CVE-2017-3939, CVE-2017-3940, CVE-2017-3941, CVE-2017-3942, CVE-2017-3943)
McAfee Network Data Loss Prevention Multiple Bugs Let Remote Users Conduct Session Hijacking and Cross-Site Scripting Attacks and Obtain Administrative Access
CVE Program record
NVD vulnerability detail

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

CVE, CWE, and OVAL are registered trademarks of [The MITRE Corporation](#) and the authoritative source of CVE content is [MITRE's CVE web site](#). This site includes MITRE data granted under the following [license](#).

Free CVE JSON API cve.report/api

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