



CVE-2017-3933

[MITRE](#)[NVD](#)[CVE.ORG](#)[JSON API](#)[Print: PDF](#)

Summary

CVE	CVE-2017-3933
State	PUBLIC
Assigner	secure@intel.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2017-10-31 14:29:00 UTC
Updated	2017-11-18 16:22:00 UTC
Description	Embedding Script (XSS) in HTTP Headers vulnerability in McAfee Network Data Loss Prevention (NDLP) 9.3.x allows remote attackers to execute arbitrary code or cause a denial of service (DoS) by sending a crafted HTTP request to the affected product. The vulnerability exists in the way the product handles the Content-Type header in the request. The product does not properly sanitize the Content-Type header, which allows an attacker to inject a malicious script. This can be used to execute arbitrary code or cause a denial of service (DoS) by sending a crafted HTTP request to the affected product. The vulnerability exists in the way the product handles the Content-Type header in the request. The product does not properly sanitize the Content-Type header, which allows an attacker to inject a malicious script. This can be used to execute arbitrary code or cause a denial of service (DoS) by sending a crafted HTTP request to the affected product.

Risk And Classification

Problem Types: CWE-79

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Mcafee	Network Data Loss Prevention	9.3.0	All	All	All
Application	Mcafee	Network Data Loss Prevention	9.3.1	All	All	All
Application	Mcafee	Network Data Loss Prevention	9.3.2	All	All	All
Application	Mcafee	Network Data Loss Prevention	9.3.3	All	All	All
Application	Mcafee	Network Data Loss Prevention	9.3.4	All	All	All
Application	Mcafee	Network Data Loss Prevention	9.3.0	All	All	All
Application	Mcafee	Network Data Loss Prevention	9.3.1	All	All	All
Application	Mcafee	Network Data Loss Prevention	9.3.2	All	All	All
Application	Mcafee	Network Data Loss Prevention	9.3.3	All	All	All
Application	Mcafee	Network Data Loss Prevention	9.3.4	All	All	All

References

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 CVE-2017-3933 Unspecified Cross Site Scripting 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.

© [CVE.report](#) 2026 |

Use of this information constitutes acceptance for use in an AS IS condition. There are NO warranties, implied or otherwise, with regard to this information or its use. Any use of this information is at the user's risk. It is the responsibility of user to evaluate the accuracy, completeness or usefulness of any information, opinion, advice or other content. EACH USER WILL BE SOLELY RESPONSIBLE FOR ANY consequences of his or her direct or indirect use of this web site. ALL WARRANTIES OF ANY KIND ARE EXPRESSLY DISCLAIMED. This site will NOT BE LIABLE FOR ANY DIRECT, INDIRECT or any other kind of loss.

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](#)