

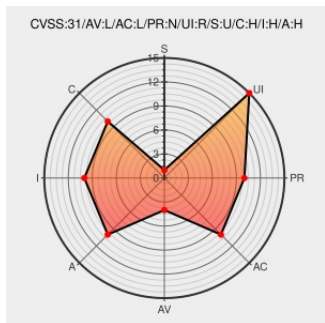


CVE-2019-1010057

Published on: 07/16/2019 12:00:00 AM UTC

Last Modified on: 05/03/2022 02:28:00 PM UTC

CVE-2019-1010057

[Source: Mitre](#)[Source: NIST](#)[CVE.ORG](#)[Print: PDF](#) 

Certain versions of [Debian Linux](#) from [Debian](#) contain the following vulnerability:

nfdump 1.6.16 and earlier is affected by: Buffer Overflow. The impact is: The impact could range from a denial of service to local code execution. The component is: nfx.c:546, nffile_inline.c:83, minilzo.c (redistributed). The attack vector is: nfdump must read and process a specially crafted file. The fixed version is: after commit

9f0fe9563366f62a71d34c92229da3432ec5cf0e.

CVE-2019-1010057 has been assigned by [GSD](#) cve-assign@distributedweaknessfiling.org to track the vulnerability - currently rated as **HIGH** severity.

Affected Vendor/Software: [GSD](#) **nfdump** - **nfdump** version $\leq$ 1.6.16 [fixed: after commit 9f0fe9563366f62a71d34c92229da3432ec5cf0e]

CVSS3 Score: **7.8 - HIGH**

Attack Vector	Attack Complexity	Privileges Required	User Interaction
LOCAL	LOW	NONE	REQUIRED
Scope	Confidentiality Impact	Integrity Impact	Availability Impact
UNCHANGED	HIGH	HIGH	HIGH

CVSS2 Score: **6.8 - MEDIUM**

Access Vector	Access Complexity	Authentication
NETWORK	MEDIUM	NONE
Confidentiality Impact	Integrity Impact	Availability Impact
PARTIAL	PARTIAL	PARTIAL

CVE References

Description	Tags	Link
[SECURITY] Fedora 30 Update: nfdump-1.6.18-1.fc30 - package-announce - Fedora Mailing-Lists	lists.fedoraproject.org text/html	 FEDORA FEDORA-2019-0fbfb00cbb
Multiple security vulnerabilities in minilzo.c, nffile_inline.c and nfx.c · Issue #104 · phaag/nfdump · GitHub	Issue Tracking Vendor Advisory github.com text/html	 MISC github.com/phaag/nfdump/issues/104
nfdump: Multiple vulnerabilities (GLSA 202003-17) — Gentoo security	security.gentoo.org text/html	 GENTOO GLSA-202003-17
[SECURITY] Fedora 29 Update: nfdump-1.6.18-1.fc29 - package-announce - Fedora Mailing-Lists	lists.fedoraproject.org text/html	 FEDORA FEDORA-2019-9013b5e75d
[SECURITY] [DLA 2383-1] nfdump security update	lists.debian.org text/html	 MLIST [debian-lts-announce] 20200926 [SECURITY] [DLA 2383-1] nfdump security update

By selecting these links, you may be leaving CVEreport webspace. We have provided these links to other websites because they may have information that would be of interest to you. No inferences should be drawn on account of other sites being referenced, or not, from this page. There may be other websites that are more appropriate for your purpose. CVEreport does not necessarily endorse the views expressed, or concur with the facts presented on these sites. Further, CVEreport does not endorse any commercial products that may be mentioned on these sites. Please address comments about any linked pages to comment@cve.report.

Related QID Numbers

500422 Alpine Linux Security Update for nfdump

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Debian	Debian Linux	9.0	All	All	All
Operating System	Fedoraproject	Fedora	29	All	All	All
Operating System	Fedoraproject	Fedora	30	All	All	All
Application	Nfdump Project	Nfdump	All	All	All	All
cpe:2.3:o:debian:debian_linux:9.0:*:*:*:*:*:						
cpe:2.3:o:fedoraproject:fedora:29:*:*:*:*:*:						
cpe:2.3:o:fedoraproject:fedora:30:*:*:*:*:*:						
cpe:2.3:a:nfdump_project:nfdump:*:*:*:*:*:						

No vendor comments have been submitted for this CVE

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](#).

CVE.report and Source URL Uptime Status [status.cve.report](#)