

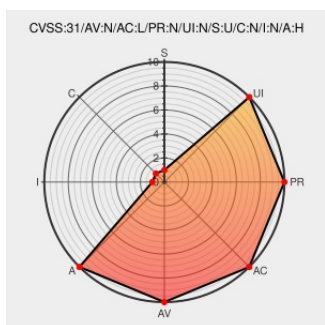


# CVE-2019-14459

Published on: 07/31/2019 12:00:00 AM UTC

Last Modified on: 11/07/2023 03:04:00 AM UTC

## CVE-2019-14459

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

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

nfdump 1.6.17 and earlier is affected by an integer overflow in the function Process\_ipfix\_template\_withdraw in ipfix.c that can be abused in order to crash the process remotely (denial of service).

CVE-2019-14459 has been assigned by [M](#) cve@mitre.org to track the vulnerability - currently rated as **HIGH** severity.

CVSS3 Score: **7.5 - HIGH**

| Attack Vector    | Attack Complexity      | Privileges Required | User Interaction    |
|------------------|------------------------|---------------------|---------------------|
| <b>NETWORK</b>   | <b>LOW</b>             | <b>NONE</b>         | <b>NONE</b>         |
| Scope            | Confidentiality Impact | Integrity Impact    | Availability Impact |
| <b>UNCHANGED</b> | <b>NONE</b>            | <b>NONE</b>         | <b>HIGH</b>         |

CVSS2 Score: **5 - MEDIUM**

| Access Vector          | Access Complexity | Authentication      |
|------------------------|-------------------|---------------------|
| <b>NETWORK</b>         | <b>LOW</b>        | <b>NONE</b>         |
| Confidentiality Impact | Integrity Impact  | Availability Impact |
| <b>NONE</b>            | <b>NONE</b>       | <b>PARTIAL</b>      |

## CVE References

| Description                                                                                 | Tags                                                                 | Link                                          |
|---------------------------------------------------------------------------------------------|----------------------------------------------------------------------|-----------------------------------------------|
| [SECURITY] Fedora 30 Update: nfdump-1.6.18-1.fc30 - package-announce - Fedora Mailing-Lists | <a href="#">lists.fedoraproject.org</a><br><a href="#">text/html</a> | <a href="#">FEDORA FEDORA-2019-0fbfb00cbb</a> |
| [SECURITY] Fedora 29 Update:                                                                | <a href="#">lists.fedoraproject.org</a>                              | <a href="#">FEDORA FEDORA-2019-9013b5e75d</a> |

nfdump-1.6.18-1.fc29 - package-announce - Fedora Mailing-Lists

text/html

Integer overflow in Process\_ipfix\_template\_withdraw (ipfix.c) · Issue #171 · phaag/nfdump · GitHub

Exploit  
Third Party Advisory  
github.com  
text/html

MISC github.com/phaag/nfdump/issues/171

Fix potential unsigned integer underflow · phaag/nfdump@3b006ed · GitHub

Patch  
Third Party Advisory  
github.com  
text/html

MISC github.com/phaag/nfdump/commit/3b006ededaf351f1723aea6c727c9edd1b1fff9b

nfdump: Multiple vulnerabilities (GLSA 202003-17) — Gentoo security

security.gentoo.org  
text/html

GENTOO GLSA-202003-17

[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](mailto: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:*****:   |                |              |         |        |         |          |

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](#)