



# CVE-2017-16844

[MITRE](#)[NVD](#)[CVE.ORG](#)[Print: PDF !\[\]\(e3f8612927870f2e0f9f5989e6dd3064\_img.jpg\)](#)

## Summary

<b>CVE</b>	CVE-2017-16844
<b>State</b>	PUBLIC
<b>Assigner</b>	cve@mitre.org
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2017-11-16 15:29:00 UTC
<b>Updated</b>	2018-02-04 02:29:00 UTC
<b>Description</b>	Heap-based buffer overflow in the loadbuf function in formisc.c in formail in procmail 3.22 allows remote attackers to cause

## Risk And Classification

**Problem Types:** CWE-119

## NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	<a href="#">Procmail</a>	<a href="#">Procmail</a>	3.22	All	All	All
Application	<a href="#">Procmail</a>	<a href="#">Procmail</a>	3.22	All	All	All

## References

Reference	Source	Link
#876511 - formail: CVE-2017-16844: heap-based buffer overflow in loadbuf() - Debian Bug report logs	MISC	<a href="https://bugs.debian.org">bugs.debian.org</a>
Procmail Buffer Overflow in formail loadbuf() Lets Remote Users Execute Arbitrary Code - SecurityTracker	SECTRACK	<a href="http://www.securitytracker.com">www.securitytrack</a>
Red Hat Customer Portal	REDHAT	<a href="https://access.redhat.com">access.redhat.cor</a>
Debian -- Security Information -- DSA-4041-1 procmail	DEBIAN	<a href="http://www.debian.org">www.debian.org</a>
[SECURITY] [DLA 1173-1] procmail security update	MLIST	<a href="https://lists.debian.org">lists.debian.org</a>
CVE Program record	CVE.ORG	<a href="http://www.cve.org">www.cve.org</a>
NVD vulnerability detail	NVD	<a href="http://nvd.nist.gov">nvd.nist.gov</a>

No vendor comments have been submitted for this CVE.

## Legacy QID Mappings

[378278](#) Virtuozzo Linux Security Update for procmail (VZLSA-2017:3269)

901165 Common Base Linux Mariner (CBL-Mariner) Security Update for procmail (7332-1)

901554 Common Base Linux Mariner (CBL-Mariner) Security Update for procmail (6803-1)

© [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](#).

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