



# CVE-2018-7873

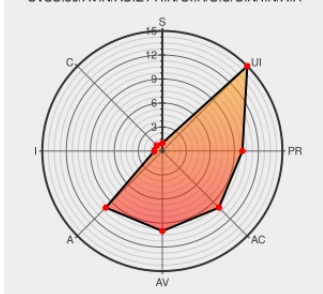
Published on: 03/08/2018 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:24:38 PM UTC

## CVE-2018-7873

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

CVSS:30/AV:N/AC:L/PR:N/UI:R/S:U/C:N/I:N/A:H



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

There is a heap-based buffer overflow in the getString function of util/decompile.c in libming 0.4.8 for INTEGER data. A Crafted input will lead to a denial of service attack.

CVE-2018-7873 has been assigned by [M](#) cve@mitre.org to track the vulnerability - currently rated as **MEDIUM** severity.

CVSS3 Score: **6.5 - MEDIUM**

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

CVSS2 Score: **4.3 - MEDIUM**

| Access Vector          | Access Complexity | Authentication      |
|------------------------|-------------------|---------------------|
| <b>NETWORK</b>         | <b>MEDIUM</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] [DLA 1386-1] ming security update | <a href="#">Mailing List</a><br><a href="#">Third Party Advisory</a><br><a href="#">lists.debian.org</a><br><a href="#">text/html</a> | <a href="#">@ MLIST [debian-lts-announce] 20180526 [SECURITY] [DLA 1386-1] ming security update</a> |

[SECURITY] Fedora 31 Update: ming-0.4.9-0.4.20181112git5009802.fc31 - package-announce - Fedora Mailing-Lists

lists.fedoraproject.org  
text/html

FEDORA FEDORA-2019-a1b6fc5274

[SECURITY] Fedora 29 Update: ming-0.4.9-0.2.20181112git5009802.fc29 - package-announce - Fedora Mailing-Lists

lists.fedoraproject.org  
text/html

FEDORA FEDORA-2019-03aa4f746c

[SECURITY] Fedora 30 Update: ming-0.4.9-0.2.20181112git5009802.fc30 - package-announce - Fedora Mailing-Lists

lists.fedoraproject.org  
text/html

FEDORA FEDORA-2019-5139453028

#892260 - Several vulnerabilities in the latest libming(0.4.8),confirm please. - Debian Bug report logs

Issue Tracking  
Third Party Advisory  
bugs.debian.org  
text/html

MISC bugs.debian.org/cgi-bin/bugreport.cgi?bug=892260

heap-buffer-overflow in function getString(util/decompile.c:346) - Issue #111 · libming/libming · GitHub

Exploit  
Third Party Advisory  
github.com  
text/html

MISC github.com/libming/libming/issues/111

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).

There are currently no QIDs associated with this CVE

| Known Affected Configurations (CPE V2.3)     |         |              |         |        |         |          |
|----------------------------------------------|---------|--------------|---------|--------|---------|----------|
| Type                                         | Vendor  | Product      | Version | Update | Edition | Language |
| Operating System                             | Debian  | Debian Linux | 7.0     | All    | All     | All      |
| Operating System                             | Debian  | Debian Linux | 7.0     | All    | All     | All      |
| Application                                  | Libming | Libming      | 0.4.8   | All    | All     | All      |
| Application                                  | Libming | Libming      | 0.4.8   | All    | All     | All      |
| cpe:2.3:o:debian:debian_linux:7.0:*:*:*:*:*: |         |              |         |        |         |          |
| cpe:2.3:o:debian:debian_linux:7.0:*:*:*:*:*: |         |              |         |        |         |          |
| cpe:2.3:a:libming:libming:0.4.8:*:*:*:*:*:   |         |              |         |        |         |          |
| cpe:2.3:a:libming:libming:0.4.8:*:*:*:*:*:   |         |              |         |        |         |          |

No vendor comments have been submitted for this CVE

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](#)