

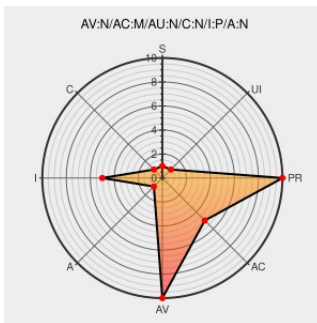


CVE-2012-2675

Published on: 07/25/2012 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:28:25 PM UTC

CVE-2012-2675

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

Certain versions of [Nedmalloc](#) from [Nedprod](#) contain the following vulnerability:

Multiple integer overflows in the (1) CallMalloc (malloc) and (2) nedpcalloc (calloc) functions in nedmalloc (nedmalloc.c) before 1.10 beta2 make it easier for context-dependent attackers to perform memory-related attacks such as buffer overflows via a large size value, which causes less memory to be allocated than expected.

CVE-2012-2675 has been assigned by secalert@redhat.com to track the vulnerability

CVSS2 Score: **4.3 - MEDIUM**

Access
Vector

NETWORK

Access
Complexity

MEDIUM

Authentication

NONE

Confidentiality
Impact

NONE

Integrity
Impact

PARTIAL

Availability
Impact

NONE

CVE References

Description

Tags

Link

oss-security - Re: memory allocator upstream patches

[www.openwall.com](http://www.openwall.com/text/html)
[text/html](#)

[MLIST \[oss-security\] 20120607 Re: memory allocator upstream patches](#)

Avoid overflowing allocation size in calloc() · ned14/nedmalloc@2965eca · GitHub

[Exploit](#)
[Patch](#)
github.com
[text/html](#)

[CONFIRM](https://github.com/ned14/nedmalloc/commit/2965eca30c408c13473c4146a9d47d547d288db1)
github.com/ned14/nedmalloc/commit/2965eca30c408c13473c4146a9d47d547d288db1

oss-security - memory allocator upstream patches

[www.openwall.com](http://www.openwall.com/text/html)
[text/html](#)

[MLIST \[oss-security\] 20120605 memory allocator upstream patches](#)

Avoid overflowing allocation size in CallMalloc() · ned14/nedmalloc@1a75975 · GitHub

[Exploit](#)
[Patch](#)
github.com
[text/html](#)

[CONFIRM](https://github.com/ned14/nedmalloc/commit/1a759756639ab7543b650a10c2d77a0ffc7a2000)
github.com/ned14/nedmalloc/commit/1a759756639ab7543b650a10c2d77a0ffc7a2000

nedmalloc/Readme.html at master · ned14/nedmalloc · GitHub

github.com
text/html

CONFIRM github.com/ned14/nedmalloc/blob/master/Readme.html

Memory allocator security revisited - Xi Wang

kqueue.org
text/html

MISC kqueue.org/blog/2012/03/05/memory-allocator-security-revisited/

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.

There are currently no QIDs associated with this CVE

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Nedprod	Nedmalloc	All	beta1	All	All
cpe:2.3:a:nedprod:nedmalloc:*:beta1:*:*:*:*:						

No vendor comments have been submitted for this CVE

← Previous ID

Next ID →