FreeNAS - Bug #41028

Patch FreeBSD CVE-2018-6922 "Resource exhaustion in TCP reassembly"

08/08/2018 08:12 AM - Alexander Motin

Status:	Done		
Priority:	No priority		
Assignee:	Alexander Motin		
Category:	OS		
Target version:	11.1-U6		
Seen in:	11.2-BETA2	**Needs Merging:**	No
Severity:	Medium	**Needs Automation:**	No
Reason for Closing:		**Support Suite Ticket:**	n/a
Reason for Blocked:		**Hardware Configuration:**	
Needs QA:	No	**ChangeLog Required:**	No
Needs Doc:	No		

Description

FreeBSD announced issue, that may be used as a method for DoS attack via specifically crafted TCP connection:
https://www.freebsd.org/security/advisories/FreeBSD-SA-18:08.tcp.asc

No data leak or corruption, only excessive CPU usage.

Related issues:

Related to FreeNAS - Bug #43558: Relax the TCP reassembly queue length limit ...	**Done**

Associated revisions

Revision 80859128 - 08/18/2018 05:39 AM - Dru Lavigne

Mention patches for recent vulnerabilities.
Ticket: #41028
Ticket: #41385
Ticket: #41772

History

#1 - 08/08/2018 08:14 AM - Alexander Motin

- Description updated

- Status changed from Unscreened to Ready for Testing

This patch supposed to mitigate issue on master: https://github.com/freenas/os/commit/f7f3a04bdea012589ed2b97fc0f0eb7d3efd0331
Stable PR: https://github.com/freenas/os/pull/137

#2 - 08/08/2018 08:17 AM - Dru Lavigne

- Needs Merging changed from Yes to No

#3 - 08/08/2018 09:42 AM - Dru Lavigne

- Target version changed from 11.2-BETA3 to 11.1-U6

#4 - 08/08/2018 09:43 AM - Dru Lavigne

- Status changed from Ready for Testing to In Progress

- Needs Merging changed from No to Yes

#5 - 08/08/2018 09:55 AM - Dru Lavigne

- Status changed from In Progress to Ready for Testing

- Needs Merging changed from Yes to No

#6 - 08/08/2018 09:55 AM - Alexander Motin

PR for 11.1-stable: https://github.com/freenas/os/pull/137

#7 - 08/08/2018 09:57 AM - Alexander Motin

The only thing can be tested there easily is presence of net.inet.tcp.reass.maxqueuelen sysctl.

#8 - 08/14/2018 09:24 AM - Bonnie Follweiler

- Status changed from Ready for Testing to Passed Testing

- Needs QA changed from Yes to No

Test Passed in FreeNAS 11.1-U6 Internal3

#10 - 08/18/2018 05:42 AM - Dru Lavigne

- Status changed from Passed Testing to Done

- Needs Doc changed from Yes to No

11.1-stable doc commit: https://github.com/freenas/freenas-docs/commit/808591286e682e0bb8e4012ce653cee2f3ce0930

#11 - 08/31/2018 10:19 AM - Alexander Motin

- Related to Bug #43558: Relax the TCP reassembly queue length limit to improve performance added