

FreeNAS - Bug #5058

devfs doesn't apply restricted rules to jail /dev mountpoint

05/23/2014 02:29 AM - Giacomo Pinagli

Status:	Resolved	
Priority:	Important	
Assignee:	John Hixson	
Category:	Middleware	
Target version:	Master - FreeNAS Nightlies	
Seen in:	9.2.1.5-RELEASE	Needs Merging: Yes
Severity:	New	Needs Automation: No
Reason for Closing:		Support Suite Ticket: n/a
Reason for Blocked:		Hardware Configuration:
Needs QA:	Yes	ChangeLog Required: No
Needs Doc:	Yes	

Description

Following this FreeBSD security advisory (<http://www.freebsd.org/security/advisories/FreeBSD-SA-14:07.devfs.asc>) I've checked all my running systems.

I run several jails on FreeNAS and some jails on a FreeBSD 10 system. Both are using The Warden.

What I found in both systems is the fact that root user in the jail (this is the default user) has unlimited access to /dev mounted in the jail by devfs which is a huge security issue.

An attacker that compromise a jails can for example format a system drive or have access to other sensitive devices like mem.

The issue can be solved by issuing: `devfs -m ${devfs_mountpoint} rule -s 4 applyset`

This is a temporary fix and it obviously resets on reboots.

Why the Warden doesn't apply the system devfs ruleset?

Associated revisions

Revision eadff4f8 - 09/01/2014 07:56 AM - John Hixson

Limit jails to a single type, but still allow templates

- While here, fix the devfs security issue
- Added new 9.3 templates, updated pkgn with them

Ticket: #5058

Ticket: #5948

Ticket: #5419

History

#1 - 05/23/2014 02:25 PM - John Hixson

- Status changed from *Unscreened* to *Screened*
- Priority changed from *Expected* to *Important*

#2 - 09/01/2014 07:58 AM - John Hixson

- *Status changed from Screened to Resolved*

Fixed in [eadff4f865ec643ea94d5fec227dc87b51e74b3f](#).

#3 - 11/22/2017 12:42 PM - Dru Lavigne

- *Target version set to Master - FreeNAS Nightlies*