Prelude-LML - Bug #243

user_id.name in ssh.rules - id 1913 expsoing name as "invalid"

07/02/2007 05:16 PM - skippylou-gmail-com -

Status:	Closed	**Start date:**	
Priority:	Normal	**Due date:**	
Assignee:	Yoann VANDOORSELAERE	**% Done:**	0%
Category:		**Estimated time:**	0.00 hour
Target version:	0.9.10.1		
Resolution:	fixed		

Description

prelude-lml-0.9.8.1

Unsure if this is intended or not, but in rule id 1913 in ssh.rules, this idmef field is currently set to:

target(0).user.user_id(0).name=$2;

which prints either illegal or invalid as opposed to the username actually in the syslog message, which would be exposed as:

target(0).user.user_id(0).name=$3;

at any rate, figured i would mention it here.

thanks,

scotto

History

#1 - 07/09/2007 02:33 PM - Yoann VANDOORSELAERE

- Status changed from New to Closed

- Resolution set to fixed

(In r9670) Fix by Scott Olihovik <skippylou@gmail.com>: invalid user.user_id(0).name assignement in SSH rule 1913 (fix #243).

#2 - 04/29/2009 02:49 PM - Yoann VANDOORSELAERE

- Project changed from PRELUDE SIEM to Prelude-LML

- Category deleted (generic)

- Target version deleted (0.9.10.1)