



System iNtrusion Analysis & Reporting Environment

SNARE Agent for Linux Version 2.0 - Release Notes

Change Log:

Name: SnareLinux-SUPP
Summary: Snare for Linux - audit subsystem control and distribution
Version: 2.0.0
Release: 0

changelog

- * Tue Aug 8 2011 David Mohr
 - Duplicate of the 1.7.0 SnareLinux Agent built for audit >= 2.0
- * Tue Aug 8 2011 David Mohr
 - Updated micro web server authentication (digest)
 - Added html entity stripping to the /events web page to prevent XSS
 - Removed MD5 string from /remote web page
 - Added cookie support for Change Tokens
 - Added POST support to micro web server
 - Added pre-submit MD5 hashing of remote access password in /remote web page
 - Extended Change Token timeout
 - Updated auditctl commands to support updated "-i" flag
 - Updated SELinux policy module
 - Thanks to Andrew Brooks, of Halock Security Labs for identifying items 2, 3 and 4
- * Tue Jul 5 2011 David Mohr
 - Bug fix for authentication event collection
 - Update SELinux policy module
- * Sat Dec 18 2010 David Mohr
 - Updated architecture identification and syscall handling
 - Added ability to pass objective filters directly to auditctl
- * Mon Jun 28 2010 David Mohr
 - Updated file permissions
 - Minor Remote Control Interface updates
 - Minor configuration checking updates
 - Security patch to prevent Cross Site Request Forgery
- * Wed Dec 17 2008 David Mohr
 - Streamlined Helper/Dispatcher comms, minor resource saving
 - Removed unnecessary regex from Dispatcher, major resource saving
 - Made all file handles hot (no buffering)
 - Improved signal handling between Helper and Dispatcher
 - Fixed potential data corruption in DispatchHelper

For more information, contact your SNARE Server Sales Representative

Contact Us:
Symtrex Inc.
264 Jane Street
Toronto, Ontario
Canada M6S 3Z2
416.769.3000 ph.
866.431.8972 Toll Free
416.769.4477 fax
snaresales@symtrex.com
www.symtrex.com
www.snare-server.com



Who's Watching Your Network?



System Intrusion Analysis & Reporting Environment

- * Fri Oct 24 2008 David Mohr
 - Completely revised file watch configuration
 - Fixed "empty fqdn/criticality" problem
 - Improved authentication event handling
 - Fixed "remove objective" bug that would delete two objectives
 - Fixed message buffering in SnareDispatchHelper
 - Fixed Display Recent Events rendering when using syslog
 - Final RHEL4 targeted release

- * Wed May 28 2008 David Mohr
 - Further improved resource handling and collection speed (SnareDispatchHelper)
 - Added support for file watches
 - Updated compliance objective templates
 - Improved objective handling including ability to drop events

- * Mon Dec 3 2007 David Mohr
 - Added support for login/logout events
 - Added support for account modification events
 - Improved resource handling and collection speed (SnareDispatchHelper)

- * Mon Aug 7 2007 David Mohr
 - Added support for compound matching elements (e.g. name=/etc/* name!=/etc/blah/*)
 - Improved authentication support for remote control interface
 - Updated SELinux policy (RHEL5 support)
 - Improved automatic audit configuration using objective returncode detection to pre filter unnecessary records
 - Fixed element matching error
 - Fixed error in criticality reporting (e.g. criticality was always zero)
 - Fixed race condition that could potentially clear all audit rules on restart
 - Improved efficiency allowing a higher throughput
 - Improved installer for easier deployment

- * Mon Jul 2 2007 David Mohr
 - Fixed syslog output
 - Added file output support to web interface
 - Fixed "Other" objective type to allow underscores
 - Fixed exclusion lists
 - Changed wildcards to match zero or more characters
 - Added regex option to config file
 - Added better Audit version detection
 - DNS timeout for restricted access hosts

- * Wed Nov 29 2006 Leigh Purdie
 - Initial release - InterSect Alliance - <http://www.intersectalliance.com/>

Contact Us:
Symtrex Inc.
264 Jane Street
Toronto, Ontario
Canada M6S 3Z2
416.769.3000 ph.
866.431.8972 Toll Free
416.769.4477 fax
snaresales@symtrex.com
www.symtrex.com
www.snare-server.com



Who's Watching Your Network?