System iNtrusion Analysis & Reporting Environment

Release Notes for Snare Epilog for Unix

About this document

This document provides release notes for the Snare Enterprise Epilog for Unix.

Snare Enterprise Epilog for Unix v1.5.7

Snare Enterprise Epilog for Unix v1.5.7 was released on 4th September 2015

Bug Fixes

- **Issue with processing files over 2GB on Solaris systems**
  An issue was found where Epilog failed to send logs to its server when the monitored log file size exceeded 2 gigabytes on Solaris systems. This update allows the agent to monitor log files that grow to be over 2GB up to the file system limitations.

Snare Enterprise Epilog for Unix v1.5.6

Snare Enterprise Epilog for Unix v1.5.6 was released on 30th June 2015

Security Fix

- **Denial of Service to Web interface on Various Snare Agents**
  Security Denial of Service vulnerability to correct malformed HTTP post exploit that can cause the agent to crash or hang.

Bug Fixes

- **Issue with reading the configuration file**
  The agent was not handling the case in situations where the Epilog service was already running, but the configuration file directory became unreadable for whatever reason (removal, no permission, disk failure etc). We now correctly handle the error condition and continue with our in-memory configuration.

- **Unix Epilog does not stop using the script correctly**
  Upon a restart of the agent, the old Epilog process would not be correctly stopped when using the scripts in /etc/init.d/epilogd. This is now fixed for this release.

Snare Enterprise Epilog for Unix v1.5.5

Snare Enterprise Epilog for Unix v1.5.5 was released on 26th February 2015

Enhancements

- **New builds available for Solaris and Linux operating systems**
  This includes Red Hat Enterprise Linux, and SUSE Linux Enterprise Desktop (SLED), Debian and Ubuntu. NOTE: Triple des encryption is only available for users with version 5 Snare Server or below.

  Builds also available for Solaris Sparc and intel available. Please note that triple des encryption is not available for these agents.

Bug Fixes

- **Unix Epilog is not using exclude and include matching correctly**
  A bug in handling Objectives caused Epilog to process filters on events in a way that was somewhat counter-intuitive to the end user.
  The following changes to Epilog make the internal rule processing match what is seen on the web interface.
  - New rules are appended to the list of objectives. Previously when a rule was added it would become the first to be processed in the defined list of objective rules.
  - When no rules are defined, Epilog will now display all events from watched files. This 'Include All by default' behavior is only when no objective rules have been defined.
  - Once an objective has been defined, Epilog will exclude all events unless a match is found in the defined objectives.